Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Романчук Иван Сергеевич
Должность: Ректор
Дата подписания: 31.10.2023 10:28:10
Уникальный программный ключ:
6319edc2b582ffdacea443f01d5779368d0957ac34f5cd074d8118153045324f9

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

АДМИНИСТРИРОВАНИЕ ОПЕРАЦИОННЫХ СИСТЕМ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Оленников Е.А. Администрирование операционных систем. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Администрирование операционных систем [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Оленников Е.А, 2020.

1. Пояснительная записка

Учебная дисциплина «Администрирование операционных систем» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Администрирование операционных систем» является изложение основополагающих принципов администрирования операционных систем (ОС) и примеров реализации подобных методов на практике.

Задачи дисциплины «Администрирование операционных систем»:

- дать представление об основных задачах администрирования ОС и методах их решения;
- научить использовать встроенные средства ОС для решения задач администрирования ОС.

1.1. Место дисциплины в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Операционные системы».

Дисциплина «Администрирование операционных систем» способствует освоению следующих дисциплин: «Защита операционных систем».

1.2.**Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)**

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-8 - способность к самоорганизации и самообразованию		знать: содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; уметь: самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;
ОПК-7: способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения		знать: основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности; основные команды, применяемые при администрировании ОС Windows, Linux, Unix; уметь: выполнять установку и конфигурирование ОС Windows, Linux, Unix;

		конфигурировать и обслуживать основные сервисы безопасности ОС; работать с технической литературой и специализированными электронными ресурсами.
ПК-8: способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы		знать: основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности; базовые задачи по обеспечению защиты ОС, вычислительных ресурсов ЭВМ и данных; уметь: выполнять задачи по ограничению доступа к объектам файловой системы в ОС Windows, Linux, Unix; определять ресурсы, подлежащие защите;
ПК-15: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы		знать: типы, версии и редакции ОС Windows, Linux, Unix; основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности; основные электронные ресурсы по теме безопасного администрирования ОС; уметь: конфигурировать и обслуживать основные сервисы безопасности ОС; определять ресурсы, подлежащие защите; работать с технической литературой и специализированными электронными ресурсами;
ПК-17: способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение		знать: типы, версии и редакции ОС Windows, Linux, Unix; основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности; основные команды, применяемые при администрировании ОС Windows, Linux, Unix;

		базовые задачи по обеспечению защиты ОС, вычислительных ресурсов ЭВМ и данных; • основные электронные ресурсы по теме безопасного администрирования ОС; уметь: выполнять установку и конфигурирование ОС Windows, Linux, Unix; выполнять задачи по управлению пользователями в ОС Windows, Linux, Unix; выполнять задачи по управлению запоминающими устройствами в ОС Windows, Linux, Unix; выполнять задачи по ограничению доступа к объектам файловой системы в ОС Windows, Linux, Unix; конфигурировать и администрировать основные сетевые службы в ОС Windows, Linux, Unix; конфигурировать и обслуживать основные сервисы безопасности ОС;
ПК-18: способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		знать: основные задачи и функции администратора ОС; основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности; основные команды, применяемые при администрировании ОС Windows, Linux, Unix; базовые задачи по обеспечению защиты ОС, вычислительных ресурсов ЭВМ и данных; уметь: выполнять установку и конфигурирование ОС Windows, Linux, Unix; конфигурировать и администрировать основные сетевые службы в ОС Windows, Linux, Unix; выполнять резервное копирование и восстановление данных в ОС Windows, Linux, Unix; конфигурировать и обслуживать основные сервисы безопасности ОС; определять ресурсы, подлежащие защите;

		работать с технической литературой и специализированными электронными ресурсами.

* не предусмотрено

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)	
		5 семестр	**6** семестр
Общий объем зач. ед.	**7**	4	3
час.	**252**	**144**	**108**
Из них:			
Часы аудиторной работы (всего):	**144**	**72**	**72**
Лекции	72	36	36
Практические занятия		0	0
Лабораторные/практические занятия по подгруппам	72	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	**108**	72	36
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		экзамен	экзамен

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной) и традиционной (5-балльной) систем оценок.

Экзаменационная оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических работ, индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должно быть сдано минимум 50% практических работ и сделан ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен сдать минимум 75% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с

другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен сдать минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами.

Примечание. Студент, желающих исправить экзаменационную оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена.4. Содержание дисциплины.

Важной составляющей освоения дисциплины «Администрирование операционных систем» является выполнение курсовой работы. Курсовая работа оценивается независимо от результатов обучения по курсу «Администрирование операционных систем». Применяется зачетная форма оценивания. Оценка за курсовую работу вносится в зачетную книжку студента в соответствующую графу.

Для получения оценки «зачет» необходимо выполнение следующих требований:

- тема курсовой работы соответствует содержанию;
- цель и задачи курсовой работы соответствуют содержанию и заявленной теме;
- цель курсовой работы достигнута, а задачи решены;
- курсовая работа соответствует требованиям к структуре и оформлению.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
Семестр 5						
1.	Введение в администрирование ОС.	6	2	0	2	0
2.	Базовые инструменты администрирования ОС Windows.	6	2	0	2	0
3.	Управление локальными пользователями в ОС Windows.	12	4	0	4	0
4.	Управление дисковыми ресурсами.	12	4	0	4	0
5.	Сетевые параметры в ОС Windows.	12	2	0	4	0
6.	Система доменных имен.	12	2	0	2	0

7.	Протокол динамической конфигурации хоста.	12	2	0	2	0
8.	Настройка файлового сервера под управлением ОС Windows.	12	2	0	2	0
9.	Администрирование доменов в сетях Windows.	12	8	0	6	0
10.	Настройка удаленного доступа в Windows.	12	2	0	2	0
11.	Резервное копирование данных.	12	2	0	2	0
12.	Мониторинг работы и контроль производительности ОС Windows.	12	2	0	2	0
13.	Автоматизация задач администрирования в ОС Windows. PowerShell.	12	2	0	2	0
	Всего (часов) за семестр 5	144	36	0	36	2
Семестр 6						
1.	Общий обзор Unix-like систем. ОС FreeBSD.	6	2	0	2	0
2.	Командная строка FreeBSD.	6	2	0	2	0
3.	Управление локальными пользователями в ОС FreeBSD.	6	2	0	2	0
4.	Управление дисковыми ресурсами, ФС UFS.	6	2	0	2	0
5.	Ограничение доступа к фалам и каталогам.	12	4	0	4	0
6.	Сетевые параметры в ОС FreeBSD.	6	2	0	2	0
7.	Загрузка ОС FreeBSD. Сборка ядра, обновление системы.	12	4	0	4	0
8.	Установка программного обеспечения в ОС FreeBSD.	6	2	0	2	0
9.	Сервер имен под управлением ОС FreeBSD.	6	2	0	2	0
10.	DHCP-сервера под управлением ОС FreeBSD.	6	2	0	2	0
11.	Файловый сервер под управлением ОС FreeBSD.	12	4	0	4	0
12.	Организация удаленного доступа к серверу под управлением ОС FreeBSD.	6	2	0	2	0
13.	Организация резервного копирования и	6	2	0	2	0

	восстановления данных в ОС FreeBSD.					
14.	Мониторинг работы и контроль производительности ОС FreeBSD.	6	2	0	2	0
15.	Обеспечение отказоустойчивости ОС FreeBSD.	6	2	0	2	0
	Всего (часов) за семестр 6	108	36	0	36	2
	Итого (часов)	252	72	0	72	4

4.2. Содержание дисциплины (*модуля*) по темам

Семестр 5.

Введение в администрирование ОС. Цели и задачи администрирования ОС. Знакомство с редакциями ОС Windows, описание процесса установки ОС Windows.

Практическая работа 1.

Установка ОС Windows Server на виртуальную машину.

Базовые инструменты администрирования ОС Windows. Реестр ОС Windows - назначение, организация. Утилиты для работы с реестром. Обзор базовых инструментов администрирования: консоль управления, оснастки.

Практическая работа 2.

Утилиты для просмотра и редактирования реестра. Знакомство с базовыми инструментами администрирования ОС Windows. Создание собственных консолей управления и панелей задач.

Управление локальными пользователями в ОС Windows. Управление учетными локальными записями. Настройка среды пользователя. Локальная групповая политика.

Практическая работа 3.

Управление локальными пользователями в ОС Windows. Создание и редактирование учетных записей пользователей и групп. Настройка среды пользователя.

Практическая работа 4.

Редактирование локальной групповой политики.

Управление дисковыми ресурсами. Методы разбиения дискового пространства (разделы, динамические тома). Файловая система NTFS. Управление доступом к файлам и папкам. Настройка квот, аудит.

Практическая работа 5.

Разметка диска. Создание томов и разделов.

Практическая работа 6.

Настройка прав доступа к файлам и папкам. Настройка дисковых квот. Аудит.

Сетевые параметры в ОС Windows. Настройка сетевых параметров. Диагностика и устранение неполадок TCP/IP. Настройка сетевого экрана.

Практическая работа 7.

Настройка сетевых параметров в ОС Windows. Изучение утилит для диагностики и устранения неполадок TCP/IP.

Практическая работа 8.

Настройка сетевого экрана.

Система доменных имен. Настройка DNS сервера под управлением ОС Windows. Утилиты командной строки для диагностики DNS-сервера.

Практическая работа 9.

Настройка DNS сервера под управлением ОС Windows. Использование утилит командной строки для диагностики DNS-сервера.

Протокол динамической конфигурации хоста. Установка и настройка DHCP-сервера.

Практическая работа 10.

Установка и настройка DHCP-сервера под управлением ОС Windows.

Настройка файлового сервера под управлением ОС Windows. Служба доступа к файлам и принтерам сетей Microsoft. Распределенная файловая система (DFS). Автономные файлы.

Практическая работа 11.

Настройка службы доступа к файлам и принтерам сетей Microsoft для предоставления совместного доступа к файлам. Работа с автономными файлами. Настройка DFS.

Администрирование доменов в сетях Windows. Служба каталогов Active Directory. Основные понятия, физическая и логическая организация домена. Базовые инструменты администрирования доменов. Создание доменов, деревьев, лесов. Управление пользователями, группами, компьютерами в домене. Управление доменными групповыми политиками.

Практическая работа 12.

Создание домена. Управление пользователями, группами, компьютерами. Создание организационных единиц.

Практическая работа 13.

Создание доменного дерева, леса. Настройка доверительных отношений.

Практическая работа 14.

Управление доменными групповыми политиками. Использование групп безопасности. Анализ и настройка безопасности. Оценка влияния групповых политик на компьютеры и пользователей домена.

Настройка удаленного доступа в Windows. Средства и методы удаленного доступа в Windows.

Практическая работа 15.

Настройка удаленного доступа в Windows.

Резервное копирование данных. Планирование архивации. Основные методы и типы резервного копирования. Архивация и восстановление данных в ОС Windows.

Практическая работа 16.

Настройка архивации данных в ОС Windows. Восстановление данных из резервной копии в ОС Windows.

Мониторинг работы и контроль производительности ОС Windows. Цель, основные подходы. Обзор инструментов мониторинга.

Практическая работа 17.

Мониторинг работы и контроль производительности ОС Windows.

Автоматизация задач администрирования в ОС Windows. PowerShell.

Практическая работа 18.

Использование PowerShell для автоматизации задач администрирования в ОС Windows.

Семестр 6.

Общий обзор Unix-like систем. ОС FreeBSD. Основные понятия и специфические особенности. Знакомство установка ОС FreeBSD. Структура и назначение каталогов.

Практическая работа 1.

Установка ОС FreeBSD на виртуальную машину.

Командная строка FreeBSD. Приемы работы, базовые операции, команды, утилиты.

Практическая работа 2.

Основные приемы работы в командной строке, перенаправление вывода, конвейеры. Основные операции с файлами и каталогами.

Управление локальными пользователями в ОС FreeBSD. Создание редактирование учетных записей пользователей и групп. Повышение привилегий. Ограничение пользователей.

Практическая работа 3.

Создание редактирование учетных записей пользователей и групп. Повышение привилегий. Ограничение пользователей.

Управление дисковыми ресурсами, ФС UFS. Представление запоминающих устройств. Методы и утилиты разметки дискового пространства. Монтирование.

Практическая работа 4.

Управление дисковыми ресурсами, ФС UFS. Методы и утилиты разметки дискового пространства. Монтирование.

Ограничение доступа к файлам и каталогам. Классический подход, ACL, флаги файлов, уровни безопасности.

Практическая работа 5.

Ограничение доступа к файлам и каталогам. Классический подход, ACL, флаги файлов, уровни безопасности.

Сетевые параметры в ОС FreeBSD. Настройка сетевых параметром. Диагностика и устранение неполадок TCP/IP.

Практическая работа 6.

Настройка сетевых параметром. Диагностика и устранение неполадок TCP/IP.

Загрузка ОС FreeBSD. Сборка ядра, обновление системы.

Загрузчики и этапы загрузки ОС FreeBSD. Конфигурирование, сборка, обновление ядра ОС. Обновление ОС.

Практическая работа 7.

Настройка процесса загрузки FreeBSD. Конфигурирование, сборка, обновление ядра ОС. Обновление ОС.

Установка программного обеспечения в ОС FreeBSD. Методы установки программного обеспечения, система портов и пакетов.

Практическая работа 8.

Установка ПО, используя систему портов и пакетов.

Сервер имен под управлением ОС FreeBSD. Конфигурирование сервера BIND.

Практическая работа 9.
Конфигурирование сервера BIND.
DHCP-сервера под управлением ОС FreeBSD. Установка и настройка DHCP-сервера.
Практическая работа 10.
Установка и настройка DHCP-сервера.

Файловый сервер под управлением ОС FreeBSD.
Настройка суперсервера, FTP. NFS, Samba.
Практическая работа 11.
Настройка суперсервера, FTP. NFS, Samba.

Организация удаленного доступа к серверу под управлением ОС FreeBSD.
Методы организации удаленного доступа. Настройка SSH.

Практическая работа 12.
Организация удаленного доступа к серверу под управлением ОС FreeBSD. Настройка SSH.

Организация резервного копирования и восстановления данных в ОС FreeBSD.
Методы и инструменты резервного копирования.

Практическая работа 13.
Настройка резервного копирования и восстановления данных в ОС FreeBSD.
Мониторинг работы и контроль производительности ОС FreeBSD. Цель, основные подходы. Обзор инструментов мониторинга. Настройка службы системной журнализации.
Практическая работа 14.
Мониторинг работы и контроль производительности ОС FreeBSD. Настройка службы системной журнализации.

Обеспечение отказоустойчивости ОС FreeBSD. Основные методы и инструменты.

Практическая работа 15.
Обеспечение отказоустойчивости ОС FreeBSD.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
Семестр 5		
1.	Введение в администрирование ОС.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
2.	Базовые инструменты администрирования ОС Windows.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

3.	Управление локальными пользователями в ОС Windows.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
4.	Управление дисковыми ресурсами.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
5.	Сетевые параметры в ОС Windows.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
6.	Система доменных имен.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
7.	Протокол динамической конфигурации хоста.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
8.	Настройка файлового сервера под управлением ОС Windows.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
9.	Администрирование доменов в сетях Windows.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
10.	Настройка удаленного доступа в Windows.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
11.	Резервное копирование данных.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
12.	Мониторинг работы и контроль производительности ОС Windows.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
13.	Автоматизация задач администрирования в ОС Windows. PowerShell.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
Семестр 6		
1.	Общий обзор Unix-like систем. ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
2.	Командная строка FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
3.	Управление локальными пользователями в ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
4.	Управление дисковыми ресурсами, ФС UFS.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
5.	Ограничение доступа к файлам и каталогам.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
6.	Сетевые параметры в ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
7.	Загрузка ОС FreeBSD. Сборка ядра, обновление системы.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
8.	Установка программного обеспечения в ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
9.	Сервер имен под управлением ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
10.	DHCP-сервера под управлением ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

11.	Файловый сервер под управлением ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
12.	Организация удаленного доступа к серверу под управлением ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
13.	Организация резервного копирования и восстановления данных в ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
14.	Мониторинг работы и контроль производительности ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
15.	Обеспечение отказоустойчивости ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение основной и дополнительной литературы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации – экзамен. Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса.

Вопросы к экзамену.

5 семестр

1. Цели и задачи администрирования ОС.
2. Основные задачи администрирования рабочей станции и сервера.
3. Сравнительная характеристика версий и редакций ОС Windows.
4. Реестр ОС Windows - назначение, организация. Утилиты для работы с реестром.
5. Инструменты администрирования в ОС Windows. Консоль управления, оснастки, панель задач. Основные оснастки и их назначение.
6. Основные задачи по управлению локальными пользователями в ОС Windows. Учетная запись. Группы. Профиль пользователя.
7. Управление локальными пользователями и группами из командной строки - основные команды.
8. Локальные групповая политика. Административные шаблоны.
9. Методы разбиения дискового пространства. Разделы, тома. Типы томов.
10. Управление доступом к файлам и каталогам в NTFS. Наследование разрешений. Дисковые квоты.
11. Задачи по обслуживанию файловой системы NTFS.
12. Настройка сетевых параметров в ОС Windows.
13. Настройка сетевого экрана.
14. Основные методы и утилиты диагностика и устранения неполадок TCP/IP.
15. Система доменных имен. Основные понятия.
16. Настройка службы DNS под управлением ОС Windows. Утилиты командной строки для диагностики DNS-сервера.
17. Служба DHCP – основные понятия. Настройка службы DHCP под управлением ОС Windows.

18. Настройка файлового сервера под управлением ОС Windows. Основные службы.
19. Службы каталогов – основные понятия. Active Directory. Логическая и физическая организация домена.
20. Основные задачи администратора домена. Инструменты администрирования домена.
21. Основные задачи по управлению доменными пользователями в ОС Windows. Доменная учетная запись. Доменные группы.
22. Доменные групповые политики. Управление групповыми политиками.
23. Резервное копирование данных - цель, методы. Планирование архивации. Типы резервных копий.
24. Архивация и восстановление данных в ОС Windows.
25. Автоматизация задач администрирования в ОС Windows. PowerShell.
26. Мониторинг работы и контроль производительности Windows Server.

6 семестр

1. Дать сравнительную характеристику нескольких Unix-like систем.
2. Основные задачи по управлению пользователями в Unix-like системе.
3. Выполнение задач от имени другого пользователя. Утилиты su, sudo.
4. Основные команды и утилиты для управления пользователями и группами пользователей в Unix-like системах.
5. Методы ограничения пользователей.
6. Методы разбиения дискового пространства. Утилиты, используемые для управления разделами.
7. Способы и параметры монтирования разделов.
8. Контроль доступа к объектам файловой системы в Unix-like системе. Смена владельца файла.
9. Настройка сетевых параметров. Диагностика и устранение неполадок TCP/IP.
10. Служба системной журнализации. Типы событий. Настройка.
11. Процесс загрузки ОС FreeBSD. Основные этапы. Дерево сценариев.
12. Конфигурирование и сборка ядра в Unix-like системе.
13. Способы обновления ОС FreeBSD.
14. Способы установки ПО в ОС FreeBSD.
15. Настройка сервера BIND в ОС FreeBSD.
16. Настройка службы DHCP-сервера ОС FreeBSD.
17. Настройка файлового сервера в ОС FreeBSD. Основные службы.
18. Организация удаленного доступа в Unix-like системе.
19. Методы резервного копирования и восстановления в Unix-like системе.
20. Мониторинг работы и контроль производительности ОС FreeBSD. Обеспечение отказоустойчивости ОС FreeBSD.

Обязательным этапом аттестации студента 5 курса является курсовая работа по дисциплине «Администрирование операционных систем». Курсовая работа является формой самостоятельной работы студента. Для ее выполнения определяется тема курсовой работы. Тему работы предлагает преподаватель, однако она может быть выбрана и предложена самим студентом по согласованию с преподавателем.

Курсовая работа выполняется в течении учебного семестра. Сроки выполнения курсовой работы устанавливаются согласно графику учебного процесса.

Курсовая работа должна строго соответствовать требованиям по оформлению и содержать следующие структурные элементы: титульный лист, содержание, введение, теоретическая и практическая часть, заключение, список используемой литературы.

Работа должна быть распечатана и в установленный срок сдана на проверку преподавателю. Преподаватель проверяет и оценивает сданную работу.

Примерная тематика курсовых работ.

- Анализ методов организации удаленного доступа к ОС с учетом требований ИБ.
- Анализ методов резервного копирования и восстановление данных в ОС.
- Аналитический обзор загрузчиков ОС; их достоинства и недостатки, структура, уязвимости, количественные характеристики и примеры применения.
- Исследование недокументированных особенностей реестра Windows.
- Разработка скриптов для автоматизации задач по администрированию ОС.
- Разработка утилит для решения задач по администрированию ОС.
- Разработка специализированных дистрибутивов.
- Разработка учебно-методических материалов по курсу «Администрирование ОС».
- Разработка измерительных материалов по курсу «Администрирование ОС».

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОК-8 - способность к самоорганизации и самообразованию	**Знает**: содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; **Умеет**: самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;	Практическая работа. Курсовая работа. Экзамен**.**	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

2.	ОПК-7: способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	**Знает**: основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности; основные команды, применяемые при администрировании ОС Windows, Linux, Unix; **Умеет**: выполнять установку и конфигурирование ОС Windows, Linux, Unix; конфигурировать и обслуживать основные сервисы безопасности ОС; работать с технической литературой и специализированными электронными ресурсами.	Практическая работа. Курсовая работа. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
3.	ПК-8: способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы	**Знает**: основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности; базовые задачи по обеспечению защиты ОС, вычислительных ресурсов ЭВМ и данных; **Умеет**: выполнять задачи по ограничению доступа к объектам файловой системы в ОС Windows, Linux, Unix; определять ресурсы, подлежащие защите;	Практическая работа. Курсовая работа. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о

				текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
4.	ПК-15: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	**Знает**: типы, версии и редакции ОС Windows, Linux, Unix; основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности; основные электронные ресурсы по теме безопасного администрирования ОС; **Умеет**: конфигурировать и обслуживать основные сервисы безопасности ОС; определять ресурсы, подлежащие защите; работать с технической литературой и специализированными электронными ресурсами;	Практическая работа. Курсовая работа. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
5.	ПК-17: способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы	**Знает**: типы, версии и редакции ОС Windows, Linux, Unix; основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности; основные команды, применяемые при администрировании ОС Windows, Linux, Unix;	Практическая работа. Курсовая работа. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных

	управления базами данных, сетевое программное обеспечение	базовые задачи по обеспечению защиты ОС, вычислительных ресурсов ЭВМ и данных; основные электронные ресурсы по теме безопасного администрирования ОС; **Умеет**: выполнять установку и конфигурирование ОС Windows, Linux, Unix; выполнять задачи по управлению пользователями в ОС Windows, Linux, Unix; выполнять задачи по управлению запоминающими устройствами в ОС Windows, Linux, Unix; выполнять задачи по ограничению доступа к объектам файловой системы в ОС Windows, Linux, Unix; конфигурировать и администрировать основные сетевые службы в ОС Windows, Linux, Unix; конфигурировать и обслуживать основные сервисы безопасности ОС;		заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
6.	ПК-18: способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства	**Знает**: основные задачи и функции администратора ОС; основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности; основные команды, применяемые при администрировании ОС Windows, Linux, Unix; базовые задачи по обеспечению защиты ОС, вычислительных ресурсов ЭВМ и данных; **Умеет**: выполнять установку и конфигурирование ОС Windows, Linux, Unix; конфигурировать и администрировать основные	Практическая работа. Курсовая работа. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем

	криптографической защиты информации	сетевые службы в ОС Windows, Linux, Unix; выполнять резервное копирование и восстановление данных в ОС Windows, Linux, Unix; конфигурировать и обслуживать основные сервисы безопасности ОС; определять ресурсы, подлежащие защите; работать с технической литературой и специализированными электронными ресурсами.		контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Айвенс, К. Администрирование Microsoft Windows Server 2003 : учебное пособие / К. Айвенс. — 2-е изд. — Москва : ИНТУИТ, 2016. — 486 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100554 (дата обращения: 15.05.2020).

7.2. Дополнительная литература:

1. Мошков, М. Е. Введение в системное администрирование Unix : учебное пособие / М. Е. Мошков. — 2-е изд. — Москва : ИНТУИТ, 2016. — 208 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100710 (дата обращения: 15.05.2020).
2. Администрирование ОС Unix : руководство. — 2-е изд. — Москва : ИНТУИТ, 2016. — 303 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100729 (дата обращения: 15.05.2020).

7.3. Интернет-ресурсы

1. вузовские электронно-библиотечные системы учебной литературы.
2. доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru.
3. https://docs.microsoft.com/
4. https://www.freebsd.org/

7.4 Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) https://icdlib.nspu.ru/
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА https://rusneb.ru/
- Справочная правовая система КонсультантПлюс http://www.consultant.ru/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Программное обеспечение виртуализации: VMWare, VirtualBox или другое.
- Операционная система Windows 7 или более поздние версии.

- Операционная система Windows Server 2012 или более поздние версии.
- Операционная система Linux, Unix-like система.
- Офисный пакет.
- Платформа для электронного обучения Microsoft Teams.

9. **Технические средства и материально-техническое обеспечение дисциплины (модуля)**

Лекционная аудитория с проектором. Компьютерный класс с установленным ПО.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

АНАЛИЗ И УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Петров И.П Анализ и управление рисками информационной безопасности. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Анализ и управление рисками информационной безопасности [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Петров И.П, 2020.

1. Пояснительная записка

Анализ и управление рисками информационной безопасности обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Основной целью дисциплины «Анализ и управление рисками информационной безопасности» является изучение методов и средств управления информационной безопасностью (ИБ) на объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта (СУИБ).

Задачи дисциплины «Анализ и управление рисками информационной безопасности»:

- познакомить студентов с основными терминами и определениями из области оценки и анализа рисков информационной безопасности;
- обучить методикам оценки и анализа рисков информационной безопасности;
- сформировать навыки построения системы управления информационной безопасностью;
- сформировать навыки построения системы управления информационными рисками.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Стандарты информационной безопасности», «Безопасность персональных данных», «Прикладные пакеты статистической обработки».

Дисциплина «Анализ и управление рисками информационной безопасности» способствует освоению следующих дисциплин: «Управление IT проектами».

1.2. **Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)**

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-8 - способность к самоорганизации и самообразованию		знает: содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; умеет: самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;
ПК-7 - способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем		знает: нормативные акты и стандарты в области управления рисками информационной безопасности; основные определения и термины из области оценки и анализа рисков информационной безопасности;

		методики оценки и анализа рисков информационной безопасности; методики разработки политики информационной безопасности; принципы построения и сопровождения системы управления информационным рисками и системы управления информационной безопасностью; умеет: определять субъекты и объекты информационной системы; составлять модель угроз и модель злоумышленника; разрабатывать политику информационной безопасности; оценивать и анализировать риски информационной безопасности; внедрять и сопровождать систему управления информационным рисками и систему управления информационной безопасностью.

* не предусмотрено

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		10 семестр
Общий объем зач. ед.	5	5
час.	180	180
Из них:		
Часы аудиторной работы (всего):	72	72
Лекции	36	36
Практические занятия	36	36
Лабораторные/практические занятия по подгруппам		
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	108	108
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		экзамен

3. Система оценивания

3.1. Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студент должен ответить на 1 вопрос из билета. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен ответить на оба вопроса

билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Определения риска информационной безопасности. Обзор различных подходов к анализу рисков информационной безопасности.	20	4	4		0
2.	Методики расчёта величины риска информационной безопасности.	20	4	4		0
3.	Управление рисками информационной безопасности.	20	4	4		0
4.	Процессный подход. Цикл Деминга-Шухарта.	20	4	4		0
5.	Обзор серий стандартов BS 7799, ISO 27000.	20	4	4		0
6.	Минимизация, ликвидация, принятие и делегирование рисков информационной безопасности	20	4	4		0
7.	Определение и структура системы управления информационными рисками.	20	4	4		0
8.	Система управления информационными рисками как фундамент системы управления	20	4	4		0

	информационной безопасностью.					
9.	Выбор и обоснование контрмер для повышения уровня защищённости информационной системы.	20	4	4		0
	Итого (часов)	180	36	36		2

4.2. Содержание дисциплины (*модуля*) по темам

Модуль 1. Риски информационной безопасности.

Тема 1. Определения риска информационной безопасности. Обзор различных подходов к анализу рисков информационной безопасности; Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний. Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Стандартизация в области построения систем управления. История развития. Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов.
Тема 2. Методики расчёта величины риска информационной безопасности. Понятие области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные подразделения организации, кадры). Описание области деятельности (структура и содержание документа). Понятие роли. Использование ролевого принципа в рамках СУИБ. Преимущества использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли). Роль высшего руководства организации в СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.). Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ.
Тема 3. Управление рисками информационной безопасности. Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Разработка Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Выбор угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ.

Модуль 2. Система управления информационной безопасностью.

Тема 4. Процессный подход. Цикл Деминга-Шухарта. Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности».

Тема 5. Обзор серий стандартов BS 7799, ISO 27000. Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации.
Тема 6. Минимизация, ликвидация, принятие и делегирование рисков информационной безопасности. Описание процесса управления рисками информационной безопасности. Описание методов минимизации, ликвидации, принятия и делегирования рисков информационной безопасности. Аутсорсинг и страхование как способы делегировать риски информационной безопасности.

Модуль 3. Система управления информационными рисками.

Тема 7. Определение и структура системы управления информационными рисками. Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения. Сложности, возникающие при внедрении процессов управления ИБ, и способы их решения. Контроль над внедрением процессов. Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа.
Тема 8. Система управления информационными рисками как фундамент системы управления информационной безопасностью. Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ. Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.
Тема 9. Выбор и обоснование контрмер для повышения уровня защищѐнности информационной системы. Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.). Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).
Планы практических занятий

Модуль 1. Риски информационной безопасности.

Тема 1. Определения риска информационной безопасности. Обзор различных подходов к анализу рисков информационной безопасности. Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO/IEC 2700x, СТО БР ИББС-1.0, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ISO/IEC 18044, ISO/IEC 25999 и др.).
Тема 2. Методики расчёта величины риска информационной безопасности. Разработка и управление политикой ИБ информационной системы
Тема 3. Управление рисками информационной безопасности. Анализ модели угроз ИБ и уязвимостей. Анализ модели информационных потоков.

Модуль 2. Система управления информационной безопасностью.

Тема 4. Процессный подход. Цикл Деминга-Шухарта; Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности».
Тема 5. Обзор серий стандартов BS 7799, ISO 27000; Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации.
Тема 6. Минимизация, ликвидация, принятие и делегирование рисков информационной безопасности. Построение системы поддержки принятия решений при управлении рисками информационной безопасности (минимизация/ ликвидация/ принятие/ делегирование).

Модуль 3. Система управления информационными рисками.
Тема 7. Определение и структура системы управления информационными рисками. Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа.
Тема 8. Система управления информационными рисками как фундамент системы управления информационной безопасностью. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.
Тема 9. Выбор и обоснование контрмер для повышения уровня защищѐнности информационной системы. Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

Образцы средств для проведения текущего контроля

1. Управление непрерывностью деятельности: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
2. Внутренние и внешние аудиты ИБ: цели и задачи процессов, сходства и различия.
3. Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ, обеспечение соответствия требованиям законодательства.
4. Документационное обеспечение СУИБ: понятия документа и записи, иерархия документов системы управления ИБ.
5. Мониторинг эффективности мер по обеспечению ИБ и процессов управления ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
6. Процессы улучшения системы управления ИБ: основные процессы, из взаимосвязь и роль в рамках СУИБ.
7. Корректирующие/предупреждающие действия: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
8. Концепция GRC-системы и её применения в процессе управления ИБ.
9. Определение и функциональные возможности ECM-систем.
10. Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС).
11. Защита автоматизированных систем управления технологическим процессом (АСУТП) и SCADA-систем.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Определения риска информационной безопасности. Обзор различных подходов к анализу рисков информационной безопасности.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
2.	Методики расчёта величины риска информационной безопасности.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
3.	Управление рисками информационной безопасности.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
4.	Процессный подход. Цикл Деминга-Шухарта.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
5.	Обзор серий стандартов BS 7799, ISO 27000.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
6.	Минимизация, ликвидация, принятие и делегирование рисков информационной безопасности	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
7.	Определение и структура системы управления информационными рисками.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
8.	Система управления информационными рисками как фундамент системы управления информационной безопасностью.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
9.	Выбор и обоснование контрмер для повышения уровня защищённости информационной системы.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение основной и дополнительной литературы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации –экзамен. Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса.

Вопросы к экзамену:

1. Процессный подход к построению СУИБ и циклическая модель PDCA.
2. Цели и задачи, решаемые СУИБ.
3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Стратегии выбора области деятельности СУИБ.
5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
6. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
7. Политика ИБ и политика СУИБ: сходства и различия.
8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
16. Внедрение процессов управления ИБ: этапы и последовательность.
17. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения.
18. Методика ITIL и ITSM: цели, задачи, примеры использования.
19. Управление рисками информационной безопасности: минимизация, ликвидация.
20. Методики оценки рисков информационной безопасности.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОК-8 - способность к самоорганизации и самообразованию	знает: содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; умеет: самостоятельно строить процесс овладения информацией, отобранной и структурированной для	Опрос на практическом занятии. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных

		выполнения профессиональной деятельности;		заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-7 - способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем	знает: нормативные акты и стандарты в области управления рисками информационной безопасности; основные определения и термины из области оценки и анализа рисков информационной безопасности; методики оценки и анализа рисков информационной безопасности; методики разработки политики информационной безопасности; принципы построения и сопровождения системы управления информационным рисками и системы управления информационной безопасностью; умеет: определять субъекты и объекты информационной системы; составлять модель угроз и модель злоумышленника; разрабатывать политику информационной безопасности; оценивать и анализировать риски информационной безопасности; внедрять и сопровождать систему управления информационным рисками и систему управления информационной безопасностью.	Опрос на практическом занятии. Экзамен.	

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

− 1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222

с. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

− 2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - Москва : ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; . - (Высшее образование). - Текст : электронный. - URL: https://znanium.com/catalog/product/402686 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

–

–

7.2. Дополнительная литература:

− 1. Бабаш, А. В. Криптографические методы защиты информации: Учебно-методическое пособие: Том 3 / Бабаш А.В., - 2-е изд. - Москва :ИЦ РИОР, НИЦ ИНФРА-М, 2014. - 216 с. (Высшее образование: Бакалавриат) - Текст : электронный. - URL: https://znanium.com/catalog/product/432654 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

− 2. Дубинин, Е. А. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - Москва : ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; + 11 с.. - (Научная мысль). - Текст : электронный. - URL: https://znanium.com/catalog/product/471787 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

–

7.3. Интернет-ресурсы

1. Вузовские электронно-библиотечные системы учебной литературы.
2. Доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru.
3. ФСБ России [Электронный ресурс]. – Режим доступа: http://fsb.ru (дата обращения 15.05.2020);
4. ФСТЭК России [Электронный ресурс]. – Режим доступа: http://fstec.ru (дата обращения 15.05.2020).

7.4 Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) https://icdlib.nspu.ru/
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА https://rusneb.ru/
- Справочная правовая система КонсультантПлюс http://www.consultant.ru/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Операционная система Windows 7 или более поздние версии.
- Операционная система Linux, Unix-like система.
- Офисный пакет.
- Платформа для электронного обучения Microsoft Teams.

9. **Технические средства и материально-техническое обеспечение дисциплины (модуля)**

Учебные аудитории для проведения лекций и практических занятий;

Лаборатории, оснащенные лабораторным оборудованием.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Паюсова Т.И. Аудит информационной безопасности. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Аудит информационной безопасности [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Паюсова Т.И., 2020.

1. Пояснительная записка

Дисциплина “Аудит информационной безопасности” направлена на освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе организации и проведения аудита информационной безопасности.

Цель дисциплины «Аудит информационной безопасности» - изучение методов и средств управления информационной безопасностью (ИБ) на объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта (СУИБ). Приобретенные знания позволят студентам основывать свою профессиональную деятельность на процессном подходе, формировать требования к системе управления ИБ конкретного объекта, принимать участие в проектировании системы управления ИБ, принимать участие в эксплуатации системы управления ИБ.

Задачи курса - изучение:

- формирования требований к системе управления ИБ конкретного объекта;
- проектирование системы управления ИБ конкретного объекта;
- эффективное управление ИБ конкретного объекта.

В процессе освоения дисциплины будут сформированы следующие компетенции:

ОПК-7 - способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

ПК-10 - способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Вариативная часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Безопасность сетевых технологий», «Администрирование операционных систем», «Основы информационной безопасности», «Операционные системы».

Дисциплина «Аудит информационной безопасности» способствует освоению следующих дисциплин: «Безопасность персональных данных», «Анализ и управление рисками информационной безопасности».

1.2.**Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)**

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОПК-7 - способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения		знать: − место и роль информационной безопасности в системе национальной безопасности Российской Федерации; − принципы построения криптографических алгоритмов, криптографические стандарты и их

		использование в информационных системах; – принципы организации информационных систем в соответствии с требованиями по защите информации. уметь: – составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные; – выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах
ПК-10 - способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		знать: – место и роль информационной безопасности в системе национальной безопасности Российской Федерации; – принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах; – принципы организации информационных систем в соответствии с требованиями по защите информации. уметь: – составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные; – выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах.

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы	**Всего часов**	**Часов в семестре** (академические часы)

	(академические часы)	**8** семестр
Общий объем зач. ед.	3	3
час.	108	108
Из них:		
Часы аудиторной работы (всего):	54	54
Лекции	18	18
Практические занятия	36	36
Лабораторные/практические занятия по подгруппам	0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	54	54
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет

3. Система оценивания

3.1. Для текущего контроля применяется 100-балльная система оценивания. Баллы проставляются за посещение практических занятий, а также активную работу на них. Результаты текущего контроля учитываются при промежуточной аттестации. Перевод баллов в зачет осуществляется по следующей шкале: от 61 до 100 баллов – «зачтено». Зачет проходит в устной форме, по билетам. В билете – 2 вопроса. Для получения оценки «зачтено» ответ студента должен показывать, что студент знает и понимает смысл и суть описываемой темы, ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Ответ может содержать небольшие недочеты.

4.1. Тематический план дисциплины

Таблица 2

№ п/п	**Наименование тем и/или разделов**	**Объем дисциплины (модуля), час.**				
		Всего	**Виды аудиторной работы** (академические часы)			**Иные виды контактной работы**
			Лекции	**Практические занятия**	**Лабораторные /практические занятия по подгруппам**	
1	2	3	4	5	6	7
Модуль 1						
1.	Базовые вопросы управления ИБ	6	2	4	0	0
2.	Процессный подход	6	2	4	0	0
3.	Область деятельности СУИБ	6	2	4	0	0
4.	Ролевая структура СУИБ	6	2	4	0	0

5.	Политика СУИБ	6	2	4	0	0
6.	Рискология ИБ	6	2	4	0	0
7.	Искажение корпоративной отчетности	6	2	4	0	0
8.	Искажение корпоративной отчетности	6	2	4	0	0
9.	Искажение корпоративной отчетности	6	2	4	0	0
	Итого (часов)	108	18	36	0	0

4.2. Содержание дисциплины (*модуля*) по темам

Модуль 1.

Тема 1. Базовые вопросы управления ИБ

Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Стандартизация в области построения систем управления. История развития.

Тема 2. Процессный подход

Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода.

Тема 3. Область деятельности СУИБ

Понятие области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные подразделения организации, кадры).

Тема 4. Ролевая структура СУИБ

Понятие роли. Использование ролевого принципа в рамках СУИБ. Преимущества использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли).

Тема 5. Политика СУИБ

Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ.

Тема 6. Рискология ИБ

Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Разработка Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Выбор угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов.

Модуль 2.

Тема 7. Основные процессы СУИБ. Обязательная документация СУИБ

Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость

процесса». Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности».

Тема 8. Внедрение разработанных процессов. Документ «Положение о применимости»

Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения. Сложности, возникающие при внедрении процессов управления ИБ, и способы их решения. Контроль над внедрением процессов.

Тема 9. Процесс «Управление инцидентами ИБ»

Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ. Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.

Тема 10. Процесс «Обеспечение непрерывности ведения бизнеса»

Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.

Модуль 3.

Тема 11. Обеспечение соответствия требованиям законодательства РФ Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.).

Тема 12. Эксплуатация и независимый аудит СУИБ

Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации.

Тема 13. Программные средства аудита ИБ Проведение анализа рисков информационной безопасности. Моделирование угроз информационной безопасности и уязвимостей. Разработка и управление политикой безопасности ИС.

Планы семинарских занятий.

Модуль 1.

Тема 1: Базовые вопросы управления ИБ

Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO/IEC 2700x, СТО БР ИББС-1.0, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ISO/IEC 18044, ISO/IEC 25999 и др.).

Тема 2: Процессный подход

Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов.

Тема 3: Область деятельности СУИБ

Описание области деятельности (структура и содержание документа).

Тема 4: Ролевая структура СУИБ

Роль высшего руководства организации в СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.).

Тема 5: Политика СУИБ

Источники информации для разработки Политики СУИБ. Описание структуры и содержания Политики СУИБ.

Тема 6: Рискология ИБ

Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ.

Модуль 2.

Тема 7: Основные процессы СУИБ. Обязательная документация СУИБ

Разработка процессов для улучшения СУИБ :

- «Внутренний аудит», «Корректирующие действия», «Предупреждающие действия».
- Процесс «Мониторинг эффективности» (включая разработку метрик эффективности).
- Понятие «Зрелость процесса».
- Процесс «Анализ со стороны высшего руководства».
- Процесс «Обучение и обеспечение осведомленности».

Тема 8: Внедрение разработанных процессов. Документ «Положение о применимости»

Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа.

Тема 9: Процесс «Управление инцидентами ИБ»

Описание процесса «Управление инцидентами ИБ».

Тема 10: Процесс «Обеспечение непрерывности ведения бизнеса»

Описание процесса «Обеспечение непрерывности ведения бизнеса».

Модуль 3.

Тема 11: Обеспечение соответствия требованиям законодательства РФ

Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

Тема 12: Эксплуатация и независимый аудит СУИБ

Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации.

Тема 13: Программные средства аудита ИБ

Проведение анализа рисков информационной безопасности. Моделирование угроз информационной безопасности и уязвимостей. Разработка и управление политикой безопасности ИС.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Базовые вопросы управления ИБ	Конспектирование и проработка лекционного материала. Работа с основной и дополнительной

		литературой. Анализ и проработка результатов практических заданий по подгруппам.
2.	Процессный подход	Конспектирование и проработка лекционного материала. Работа с основной и дополнительной литературой. Анализ и проработка результатов практических заданий по подгруппам.
3.	Область деятельности СУИБ	Конспектирование и проработка лекционного материала. Работа с основной и дополнительной литературой. Анализ и проработка результатов практических заданий по подгруппам.
4.	Ролевая структура СУИБ	Конспектирование и проработка лекционного материала. Работа с основной и дополнительной литературой. Анализ и проработка результатов практических заданий по подгруппам.
5.	Политика СУИБ	Конспектирование и проработка лекционного материала. Работа с основной и дополнительной литературой. Анализ и проработка результатов практических заданий по подгруппам.
6.	Рискология ИБ	Конспектирование и проработка лекционного материала. Работа с основной и дополнительной литературой. Анализ и проработка результатов практических заданий по подгруппам.
7.	Основные процессы СУИБ	Конспектирование и проработка лекционного материала. Работа с основной и дополнительной литературой. Анализ и проработка результатов практических заданий по подгруппам.
8.	Внедрение разработанных процессов	Конспектирование и проработка лекционного материала. Работа с основной и дополнительной литературой. Анализ и проработка результатов практических заданий по подгруппам.
9.	Процесс «Управление инцидентами ИБ»	Конспектирование и проработка лекционного материала. Работа с основной и дополнительной литературой. Анализ и проработка результатов практических заданий по подгруппам.

Порядок выполнения каждого вида самостоятельной работы:

1. Конспектирование и проработка лекционного материала.
2. Работа с основной и дополнительной литературой.
3. Анализ и проработка результатов практического занятия.
4. Подготовка доклада.

Контроль за самостоятельной работой осуществляется во время лекционных и практических занятий, а также во время финального испытания (зачет).

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Вопросы к зачету

1. Процессный подход к построению СУИБ и циклическая модель PDCA.

2. Цели и задачи, решаемые СУИБ.
3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Стратегии выбора области деятельности СУИБ.
5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
6. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
7. Политика ИБ и политика СУИБ: сходства и различия.
8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
16. Внедрение процессов управления ИБ: этапы и последовательность.
17. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения.

Примерные темы докладов:
a. Аудит ИБ.
b. Стандарты СУИБ.
c. Сертификация в сфере ИБ.
d. Направления ИБ.
e. Анализ рисков ИБ.
f. Оценка рисков ИБ.
g. Психология восприятия рисков ИБ.
h. Моделирование угроз ИБ.
i. Программные средства аудита ИБ.
j. SaaS-решение для аудита ИБ.
k. Инциденты ИБ.
l. DLP.
m. BYOD.
n. Облачная безопасность.
o. Тесты на проникновение.
p. Безопасность крупных спортивных мероприятий.
q. Безопасность АСУ ТП.
r. Управление непрерывностью деятельности: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
s. Внутренние и внешние аудиты ИБ: цели и задачи процессов, сходства и различия.
t. Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ, обеспечение соответствия требованиям законодательства.
u. Документационное обеспечение СУИБ: понятия документа и записи, иерархия документов системы управления ИБ.

v. Мониторинг эффективности мер по обеспечению ИБ и процессов управления ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
w. Процессы улучшения системы управления ИБ: основные процессы, их взаимосвязь и роль в рамках СУИБ.
x. Корректирующие/предупреждающие действия: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
Задания к практическим занятиям по подгруппам проводятся с использованием раздаточного материала, оформленного в виде учебно-методических пособий по предмету. Материал содержит теоретическую базу, задания и примеры для самопроверки.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (из паспорта компетенций)*	Оценочные материалы	Критерии оценивания
1.	ОПК-7 - способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	знать: − место и роль информационной безопасности в системе национальной безопасности Российской Федерации; − принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах; − принципы организации информационных систем в соответствии с требованиями по защите информации. уметь: − составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;	Практические работы по подгруппам, собеседования, доклад, вопросы к зачету	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п.4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

		– выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах		
2.	ПК-10 - способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	знать: – место и роль информационной безопасности в системе национальной безопасности Российской Федерации; – принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах; – принципы организации информационных систем в соответствии с требованиями по защите информации. уметь: – составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные; – выбирать необходимые инструментальные средства для разработки программ в различных	Практические работы по подгруппам, собеседования, доклад, вопросы к зачету	

		операционных системах и средах		

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. **Шаньгин, В.Ф.** Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

7.2. Дополнительная литература:

1. **Попов, И.И.** Информационная безопасность: Учебное пособие [Электронный ресурс] / Партыка Т. Л., Попов И. И., 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРАМ, 2016. - 432 с. – Режим доступа: http://znanium.com/bookread2.php?book=516806 (дата обращения 15.05.2020);
2. **Ревнивых, А.В.** Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Новосибирск : Новосибирский государственный университет экономики и управления «НИНХ», 2018. — 84 c. — ISBN 978-5-7014-0841-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/95200.html (дата обращения: 29.05.2020). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/95200

7.3. Интернет-ресурсы

- Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [On-line] (дата обращения: 15.05.2020).

7.4 Современные профессиональные базы данных и информационные справочные системы:

- Национальная электронная библиотека. - https://rusneb.ru/ [On-line] (дата обращения: 15.05.2020).

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Лицензионное ПО:**
  платформа для электронного обучения Microsoft Teams;
  MS Visual Studio;
  MS SQL Server.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

- лекционная аудитория с проектором;
- компьютерный класс.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

ВВЕДЕНИЕ В ТЕОРИЮ ВЕРОЯТНОСТЕЙ И МАТЕМАТИЧЕСКУЮ СТАТИСТИКУ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Иванов Д. И. Введение в теорию вероятностей и математическую статистику. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 «Компьютерная безопасность», утвержденного Приказом Министерства образования и науки РФ от 22.02.2018 №125.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Введение в теорию вероятностей и математическую статистику [электронный ресурс] / Режим доступа: https://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Иванов Д. И., 2020.

1. Пояснительная записка

Цели и задачи дисциплины:

Целью изучения данной дисциплины является знакомство студентов с основными понятиями, методами и результатами теории вероятностей и математической статистики. Объектами изучения в данной дисциплине являются случайные события и случайные величины. С их помощью могут быть сформулированы как законы природы, так и разнообразные процессы, происходящие в экономике, природе, технике. Отсюда объективная важность теории вероятностей и математической статистики как средства изучения случайных явлений и процессов. Задачами является изучение различных вероятностных моделей случайных событий, свойств распределений случайных величин, предельных теорем, основных задач математической статистики. Большое внимание уделяется вопросам построения математических моделей случайных экспериментов, проверке статистических гипотез, выявлению взаимосвязей между исследуемыми признаками и выработке навыков применения изученных методов при решении практических задач.

1.1. Место дисциплины в структуре образовательной программы

Дисциплина относится к блоку Б1 дисциплин обязательной части.

Для успешного освоения дисциплины студенты должны обладать знаниями и умениями, полученными при изучении курса «Высшая математика».

На основе приобретенных знаний формируются умения применять математические методы при решении профессиональных задач повышенной сложности, владеть методами построения математической модели профессиональных задач и содержательной интерпретации полученных результатов.

Знание основ высшей математики может существенно помочь в научно-исследовательской работе

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины

Код и наименование компетенции (из ФГОС ВО)	Компонент (знаниевый/функциональный)
Способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов. (ОПК-2)	Знает основные понятия, теоремы и методы алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, использующихся при изучении общетеоретических и специальных дисциплин учебного цикла; Умеет использовать знания фундаментальных основ, подходы и методы математики при решении прикладных задач; пользоваться источниками для самостоятельного изучения специальной литературы;
Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные	Знает: основные приемы решения задач обработки текстовой и числовой информации; основные способы и принципы представления структур данных; Умеет: выполнять основные этапы реализации программ на компьютере;

отчеты, обзоры по результатам выполнения исследований. (ПК-2)	реализовывать подходы процедурного программирования, реализацию вызова процедур в языках с блочной структурой.
Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем. (ПК-4)	Знает: угрозы информационной безопасности информации и модели нарушителя в АС, криптографические, программно-аппаратные и технические средства и методы защиты АС; Умеет: разрабатывать и исследовать АС

1.3. Перечень планируемых результатов освоения дисциплины (модуля):

В результате изучения дисциплины студент должен:

знать:

основные понятия, теоремы и методы теории вероятностей, математической статистики, использующихся при изучении общетеоретических и специальных дисциплин учебного цикла;

основные приемы решения задач обработки текстовой и числовой информации;

основные способы и принципы представления структур данных;

угрозы информационной безопасности информации и модели нарушителя в АС, криптографические, программно-аппаратные и технические средства и методы защиты АС;

уметь:

использовать знания фундаментальных основ, подходы и методы математики при решении прикладных задач;

пользоваться источниками для самостоятельного изучения специальной литературы;

выполнять основные этапы реализации программ на компьютере;

реализовывать подходы процедурного программирования, реализацию вызова процедур в языках с блочной структурой;

разрабатывать и исследовать АС

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Часов в семестре**
			3 семестр
Общая трудоемкость	**зач. ед.**	3	3
	час	108	108
Из них:			
Часы аудиторной работы (всего):		72	72
Лекции		36	36
Практические занятия		36	36
Лабораторные / практические занятия по подгруппам		0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося		36	36
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Экзамен

3. Система оценивания

В течение каждого семестра студенты выполняют по 3 контрольные работы и могут набрать по 20 баллов за каждую, по окончании каждого семестра планируется проведение коллоквиума по теоретическому материалу (40 баллов).

Студенты, получившие по итогам работы в семестре не менее 61 балла, получают оценку за экзамен по дисциплине автоматически в соответствии со шкалой перевода баллов в оценки: 61-75 баллов - удовлетворительно; 76-90 баллов - хорошо; 91-100 баллов - отлично.

Студенты, не получившие оценку за экзамен по дисциплине автоматически, или желающие улучшить полученную оценку, должны сдавать экзамен.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№	Наименование тем	Объем дисциплины, час.			
		Всего	Виды аудиторной работы (академические часы)		Иные виды контактной работы
			Лекции	Практические занятия	
1	2	3	4	5	6
1	Основные понятия теории вероятностей	2	2	0	
2	Случайные события.	2	0	2	
3	Классическое, геометрическое, статистическое и аксиоматическое определения вероятности события.	2	2	0	
4	Классическое, геометрическое определения вероятности.	4	0	2	
5	Условная вероятность. Теоремы сложения и умножения вероятностей.	2	2	0	
6	Условная вероятность.	2	0	2	
7	Формула полной вероятности. Формула Байеса.	4	2	0	
8	Полная вероятность.	2	0	2	
9	Схема Бернулли.	2	2	0	
10	Формула Бернулли.	2	0	2	
11	Случайные величины.	2	2	0	
12	Консультация по Блоку.	2	0	0	
13	Контрольная работа №1.	4	0	2	
14	Дискретные случайные величины. (лекция)	2	2	0	
15	Дискретные случайные величины.	2	0	2	
16	Непрерывные случайные величины. (лекция)	2	2	0	
17	Непрерывные случайные величины	2	2	2	
18	Примеры распределений известных случайных величин.	2	2	2	
19	Законы распределения.	2	0	2	
20	Числовые характеристики случайных величин.	2	2	0	
21	Характеристики случайных величин.	2	0	2	
22	Закон больших чисел.	2	2	0	

23	ЗБЧ.	4	0	2	
24	Центральная предельная теорема.	2	2	0	
25	Консультация по Блоку.	2	0	0	
26	Контрольная работа №2.	4	0	2	
27	Генеральная совокупность.	2	2	0	
28	Выборки.	2	0	2	
29	Основные выборочные характеристики	2	2	0	
30	Выборочные характеристики..	2	0	2	
31	Статистические оценки. (лекция)	4	2	0	
32	Статистические оценки.	2	0	2	
33	Методы статистического оценивания.	2	2	0	
34	Статистическое оценивание.	4	0	2	
35	Статистическая проверка гипотез.	2	2	0	
36	Консультация по Блоку.	2	0	0	
37	Контрольная работа №3.	4	0	2	
38	Консультация по Блоку.	2	0	0	
39	Коллоквиум.	12	0	0	
40	Консультация перед экзаменом.	2	0	0	
41	Экзамен по курсу.	2	0	0	
	Итого (часов)	108	36	36	2

4.2. Содержание дисциплины *(модуля)* по темам

1. **"Основные понятия теории вероятностей"**

Действия над событиями. Основные понятия: опыт, эксперимент, элементарный исход, случайные события, достоверное и невозможное события. Действия над событиями: объединение и пересечение событий, совместные и несовместные события, полная группа событий, противоположные события, свойства операций над событиями.

2. **"Случайные события."**

Действия над событиями: объединение и пересечение событий, совместные и несовместные события, полная группа событий, противоположные события, свойства операций над событиями.

3. **"Классическое, геометрическое, статистическое и аксиоматическое определения вероятности события."**

Классическое, геометрическое определения вероятности. Относительная частота появления события. Свойство устойчивости относительных частот. Статистическая вероятность. Аксиоматическое определение вероятности, свойства.

4. **"Классическое, геометрическое определения вероятности."**

Классическое, геометрическое определения вероятности. Решение задач по теме.

5. **"Условная вероятность. Теоремы сложения и умножения вероятностей."**

Теоремы сложения и умножения вероятностей. Теоремы сложения вероятностей для несовместных и совместных событий. Условная вероятность. Независимые и зависимые случайные события. Теоремы умножения для зависимых и независимых событий.

6. **"Условная вероятность."**

Теоремы сложения и умножения вероятностей. Теоремы сложения вероятностей для несовместных и совместных событий. Условная вероятность. Независимые и зависимые случайные события. Теоремы умножения для зависимых и независимых событий. .

7. **"Формула полной вероятности. Формула Байеса."**

Формула полной вероятности. Формула Байеса. Априорные и апостериорные вероятности.

8. **"Полная вероятность."**

Формула полной вероятности. Формула Байеса. Априорные и апостериорные вероятности.

9. **"Схема Бернулли."**

Формула Бернулли Наивероятнейшее число появления события в независимых испытаниях. Асимптотические приближения формулы Бернулли: формула Пуассона, локальная и интегральная формулы Муавра-Лапласа.

10. **"Формула Бернулли."**

Схема Бернулли. Формула Бернулли Наивероятнейшее число появления события в независимых испытаниях. Асимптотические приближения формулы Бернулли: формула Пуассона, локальная и интегральная формулы Муавра-Лапласа

11. **"Случайные величины."**

Определение случайной величины. Функция распределения, определение, свойства.

12. **"Консультация по Блоку."**

13. **"Контрольная работа №1."**

14. **"Дискретные случайные величины." (лекция)**

Определение дискретной случайной величины. Ряд распределения дискретной случайной величины. Функция распределения дискретной случайной величины. Способы задания: таблица распределения вероятностей, функция распределения и ее свойства, многоугольник распределения, аналитическое задание (по формуле). Математические операции над дискретными случайными величинами.

15. **"Дискретные случайные величины."**

Дискретные случайные величины. Ряд распределения дискретной случайной величины. Функция распределения дискретной случайной величины. Математические операции над дискретными случайными величинами.

16. **"Непрерывные случайные величины." (лекция)**

Непрерывные случайные величины. Определение, функция распределения непрерывной случайной величины. Функция плотности вероятностей, свойства.

17. **"Непрерывные случайные величины"**

Непрерывные случайные величины. Определение, функция распределения непрерывной случайной величины. Функция плотности вероятностей, свойства.

18. **"Примеры распределений известных случайных величин."**

Дискретные законы распределения: Бернулли, биномиальный, Пуассона, геометрический. Непрерывные законы распределений: равномерный, нормальный, показательный.

19. **"Законы распределения."**

Примеры распределений известных случайных величин. Дискретные законы распределения: Бернулли, биномиальный, Пуассона, геометрический. Непрерывные законы распределений: равномерный, нормальный, показательный.

20. **"Числовые характеристики случайных величин."**

Основные числовые характеристики случайных величин – математическое ожидание, дисперсия, среднее квадратическое отклонение, мода, медиана, квантили, центральные и начальные моменты. Характеристики формы распределения: асимметрия и эксцесс.

21. **"Характеристики случайных величин."**

Математическое ожидание, дисперсия, среднее квадратическое отклонение, мода, медиана, квантили, центральные и начальные моменты. Характеристики формы распределения: асимметрия и эксцесс.

22. **"Закон больших чисел. "**

Неравенства Маркова и Чебышева. Закон больших чисел в форме Чебышева, Бернулли, следствия.

23. **"ЗБЧ."**

Типы сходимостей последовательностей случайных величин: почти наверно, по вероятности, в среднем порядке . Неравенства Маркова и Чебышева. ЗБЧ и его различные формы. ЗБЧ в форме Чебышева, Бернулли, следствия.

24. **"Центральная предельная теорема."**

Центральная предельная теорема. Интегральная и локальная теоремы Муавра-Лапласа. Теорема Пуассона.

25. **"Консультация по Блоку."**

26. **"Контрольная работа №2."**

27. **"Генеральная совокупность."**

Выборка из генеральной совокупности и основные способы организации выборки. Группированные выборочные данные. Типы выборок. Способы отбора.

28. **"Выборки."**

Генеральная совокупность, выборка из нее и основные способы организации выборки. Группированные выборочные данные. Типы выборок. Способы отбора.

29. **"Основные выборочные характеристики"**

Основные выборочные характеристики. Эмпирические функция распределения, относительные частоты, плотность распределения. Эмпирические аналоги характеристик рассеивания случайной величины. Выборочные коэффициенты асимметрии и эксцесса. Эмпирические и выравнивающие частоты.

30. **"Выборочные характеристики."**

Эмпирические функция распределения, относительные частоты, плотность распределения. Эмпирические аналоги характеристик рассеивания случайной величины. Выборочные коэффициенты асимметрии и эксцесса. Эмпирические и выравнивающие частоты.

31. **"Статистические оценки." (лекция)**

Статистические оценки, их основные свойства. Статистическая устойчивость выборочных характеристик. Статистики, статистические оценки, их основные свойства: состоятельность, несмещенность, эффективность.

32. **"Статистические оценки."**

Статистические оценки, их основные свойства. Статистическая устойчивость выборочных характеристик. Статистики, статистические оценки, их основные свойства: состоятельность, несмещенность, эффективность.

33. **"Методы статистического оценивания."**

Методы статистического оценивания. Функция правдоподобия. Метод максимального правдоподобия, метод моментов. Точечные и интервальные оценки.

34. **"Статистическое оценивание."**

Методы статистического оценивания. Функция правдоподобия. Метод максимального правдоподобия, метод моментов. Точечные и интервальные оценки.

35. **"Статистическая проверка гипотез."**

Статистическая проверка гипотез. Основные типы гипотез. Общая логическая схема построения статистического критерия. Подбор теоретического распределения. Критерии согласия.

36. **"Консультация по Блоку."**

37. **"Контрольная работа №3."**

38. **"Консультация по Блоку."**

39. **"Коллоквиум."**

40. **"Консультация перед экзаменом."**

41. **"Экзамен по курсу."**

Средства для проведения текущего контроля

Семестр 2.

Контрольная работа №1 (примерный вариант):

1. Из букв слова «треугольник» наугад составляется пятибуквенное слово. Найти вероятность того, что получится слово «уголь».

2. Молодой саженец сосны в год прибавляет в высоту от 7 см до 15 см. Какова вероятность, что за два года его высота увеличится более чем на 17 см?

3. В квартире 4 электролампочки. Для каждой лампочки вероятность того, что она останется исправной в течение года, равна 5/6. Какова вероятность того, что в течение года придется заменить не меньше половины лампочек?

4. Среди клиентов банка 80% являются физическими лицами и 20% – юридическими. Из практики известно, что 40% всех операций приходится на долгосрочные расчеты, в то же время из общего числа операций, связанных с физическими лицами, 30% приходится на долгосрочные расчеты. Какова вероятность того, что наудачу выбранный клиент является юридическим лицом и осуществляет долгосрочный расчет?

5. В группе из 10 студентов, пришедших на экзамен, 3 подготовлены отлично (знают 20 вопросов из 20), 4 – хорошо (знают 16 вопросов из 20), 2 – посредственно (знают 10 вопросов), 1 – плохо (знает 5 вопросов). Наугад вызванный студент ответил на три произвольно заданных вопроса. Найти вероятность того, что он подготовлен плохо.

Контрольная работа №2 (примерный вариант):

1. Производится три независимых выстрела с вероятностью попадания 0,7 при каждом выстреле. Случайная величина – число попаданий в мишень. Для этой случайной величины составить закон распределения, найти и построить функцию распределения, многоугольник распределения. Найти математическое ожидание и дисперсию.
2. Непрерывная случайная величина задана плотностью распределения:

   Найти коэффициент функцию распределения, построить графики , . Найти математическое ожидание и дисперсию.
3. Известно, что случайная величина распределена по закону Пуассона с неизвестным параметром и вероятность. Найти параметр этого распределения.
4. В урне 20 белых и 100 черных шаров. Произвели выборку (с возвращением) 60 шаров. Оценить вероятность того, что число белых шаров в выборке от 3 до 17.

Контрольная работа №3 (примерный вариант):

1. Поставить гипотезу о теоретическом распределении генеральной совокупности, выбирая из трех распределений: равномерное, нормальное, показательное.
2. Найти параметры выбранного теоретического распределения.
3. С помощью критерия Пирсона (или для нормального распределения – критерия Романовского) проверить согласованность выбранного теоретического распределения с данными выборки на уровне значимости .
4. Построить график теоретической плотности распределения.

Вопросы к коллоквиуму:

1. Вероятностное пространство. Аксиомы теории вероятностей.
2. Следствия из аксиом вероятности.
3. Классическая схема вероятностного пространства.
4. Геометрическая схема вероятностного пространства.
5. Условные вероятности. Независимые события.
6. Формула полной вероятности. Формула Байеса.
7. Схема Бернулли. Предельные случаи схемы Бернулли.
8. Случайная величина. Функция распределения и ее свойства.
9. Абсолютно непрерывные и дискретные распределения.
10. Типовые распределения: биномиальное, Пуассоновское, геометрическое, равномерное, показательное, нормальное.
11. Нормальная кривая. Правило трех сигм.

12. Независимые случайные величины. Критерии независимости.
13. Математическое ожидание случайной величины и его свойства.
14. Дисперсия случайной величины и ее свойства.
15. Математическое ожидание и дисперсия типовых распределений.
16. Неравенства Маркова и Чебышева.
17. Закон больших чисел. Теорема Чебышева.
18. Центральная предельная теорема.
19. Предельные теоремы Муавра-Лапласа.
20. Группированные выборочные данные.
21. Основные выборочные характеристики. Эмпирические функция распределения, относительные частоты, плотность распределения.
22. Эмпирические аналоги характеристик рассеивания случайной величины. Выборочные коэффициенты асимметрии и эксцесса.
23. Эмпирические и выравнивающие частоты.
24. Статистические оценки, их основные свойства.
25. Методы статистического оценивания.
26. Статистическая проверка гипотез. Основные типы гипотез.
27. Общая логическая схема построения статистического критерия.
28. Подбор теоретического распределения. Критерии согласия.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ Темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1	Основные понятия теории вероятностей	Чтение обязательной и дополнительной литературы
2	Случайные события.	Проработка лекций
3	Классическое, геометрическое, статистическое и аксиоматическое определения вероятности события.	Чтение обязательной и дополнительной литературы
4	Классическое, геометрическое определения вероятности.	Проработка лекций
5	Условная вероятность. Теоремы сложения и умножения вероятностей.	Чтение обязательной и дополнительной литературы
6	Условная вероятность.	Проработка лекций
7	Формула полной вероятности. Формула Байеса.	Чтение обязательной и дополнительной литературы
8	Полная вероятность.	Проработка лекций
9	Схема Бернулли.	Чтение обязательной и дополнительной литературы
10	Формула Бернулли.	Проработка лекций
11	Случайные величины.	Чтение обязательной и дополнительной литературы
12	Консультация по Блоку.	Самостоятельное изучение заданного материала
13	Контрольная работа №1.	Проработка лекций
14	Дискретные случайные величины. (лекция)	Чтение обязательной и дополнительной литературы

15	Дискретные случайные величины.	Проработка лекций
16	Непрерывные случайные величины. (лекция)	Чтение обязательной и дополнительной литературы
17	Непрерывные случайные величины	Проработка лекций
18	Примеры распределений известных случайных величин.	Чтение обязательной и дополнительной литературы
19	Законы распределения.	Проработка лекций
20	Числовые характеристики случайных величин.	Чтение обязательной и дополнительной литературы
21	Характеристики случайных величин.	Проработка лекций
22	Закон больших чисел.	Чтение обязательной и дополнительной литературы
23	ЗБЧ.	Проработка лекций
24	Центральная предельная теорема.	Чтение обязательной и дополнительной литературы
25	Консультация по Блоку.	Самостоятельное изучение заданного материала
26	Контрольная работа №2.	Проработка лекций
27	Генеральная совокупность.	Чтение обязательной и дополнительной литературы
28	Выборки.	Проработка лекций
29	Основные выборочные характеристики	Чтение обязательной и дополнительной литературы
30	Выборочные характеристики..	Проработка лекций
31	Статистические оценки. (лекция)	Чтение обязательной и дополнительной литературы
32	Статистические оценки.	Проработка лекций
33	Методы статистического оценивания.	Чтение обязательной и дополнительной литературы
34	Статистическое оценивание.	Проработка лекций
35	Статистическая проверка гипотез.	Чтение обязательной и дополнительной литературы
36	Консультация по Блоку.	Самостоятельное изучение заданного материала
37	Контрольная работа №3.	Проработка лекций
38	Консультация по Блоку.	Самостоятельное изучение заданного материала
39	Коллоквиум.	Самостоятельное изучение заданного материала
40	Консультация перед экзаменом.	Самостоятельное изучение заданного материала
41	Экзамен по курсу.	Самостоятельное изучение заданного материала

6. Промежуточная аттестация по дисциплине

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине
5.Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)

Вопросы к экзамену.

1. Вероятностное пространство. Аксиомы теории вероятностей.
2. Следствия из аксиом вероятности.
3. Классическая схема вероятностного пространства.
4. Геометрическая схема вероятностного пространства.
5. Условные вероятности. Независимые события.
6. Формула полной вероятности. Формула Байеса.
7. Схема Бернулли. Предельные случаи схемы Бернулли.
8. Случайная величина. Функция распределения и ее свойства.
9. Абсолютно непрерывные и дискретные распределения.
10. Типовые распределения: биномиальное, Пуассоновское, геометрическое, равномерное, показательное, нормальное.
11. Нормальная кривая. Правило трех сигм.
12. Независимые случайные величины. Критерии независимости.
13. Математическое ожидание случайной величины и его свойства.
14. Дисперсия случайной величины и ее свойства.
15. Математическое ожидание и дисперсия типовых распределений.
16. Неравенства Маркова и Чебышева.
17. Закон больших чисел. Теорема Чебышева.
18. Центральная предельная теорема.
19. Предельные теоремы Муавра-Лапласа.
20. Группированные выборочные данные.
21. Основные выборочные характеристики. Эмпирические функция распределения, относительные частоты, плотность распределения.
22. Эмпирические аналоги характеристик рассеивания случайной величины. Выборочные коэффициенты асимметрии и эксцесса.
23. Эмпирические и выравнивающие частоты.
24. Статистические оценки, их основные свойства.
25. Методы статистического оценивания.
26. Статистическая проверка гипотез. Основные типы гипотез.
27. Общая логическая схема построения статистического критерия.
28. Подбор теоретического распределения. Критерии согласия.

6.2 Критерии оценивания компетенция:

Таблица 4

Карта критериев оценивания компетенций

№ п/п	Код и наименование компетенции	Оценочные материалы	Критерии оценивания
1.	Способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов. (ОПК-2).	Контрольная работа Коллоквиум Экзамен	В течение семестра студенты выполняют 3 контрольные работы и могут набрать по 20 баллов за каждую, по окончании семестра планируется проведение коллоквиума по теоретическому материалу (40 баллов). Студенты, получившие по итогам работы в семестре не менее 61 балла, получают оценку за экзамен по дисциплине автоматически в

2.	Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований. (ПК-2)	Контрольная работа Коллоквиум Экзамен	соответствии со шкалой перевода баллов в оценки: 61-75 баллов - удовлетворительно; 76-90 баллов - хорошо; 91-100 баллов - отлично. Студенты, не получившие оценку за экзамен по дисциплине автоматически, или желающие улучшить полученную оценку, должны сдавать экзамен. Экзамен оценивается по принятой в ТюмГУ шкале (2-5). Оценка ответа студента на экзаменационный билет зависит от правильности и полноты изложения материала, от умения привести примеры, иллюстрирующие теоретические положения, а также от наличия или отсутствия математических и методических ошибок при выполнении практических заданий.
3.	Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем. (ПК-4)	Контрольная работа Коллоквиум Экзамен	

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература:

1. Кацман, Ю. Я. Теория вероятностей, математическая статистика и случайные процессы: Учебник / Кацман Ю.Я. - Томск:Изд-во Томского политех. университета, 2013. - 131 с.: ISBN 978-5-4387-0173-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/673043 (дата обращения: 28.05.2020). – Режим доступа: по подписке.

7.2 Дополнительная литература:

1. Бочаров, П. П. Теория вероятностей. Математическая статистика [Электронный ресурс] / П. П. Бочаров, А. В. Печинкин. - 2-е изд. - Москва : ФИЗМАТЛИТ, 2005. - 296 с. - ISBN 5-9221-0633-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/405754 (дата обращения: 28.05.2020). – Режим доступа: по подписке.

2. Павлов, С. В. Теория вероятностей и математическая статистика: Учебное пособие / С.В. Павлов. - Москва : ИЦ РИОР: ИНФРА-М, 2010. - 186 с. (Карманное учебное пособие). ISBN 978-5-369-00679-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/217167 (дата обращения: 28.05.2020). – Режим доступа: по подписке.

7.3 Интернет-ресурсы:

1. Art of Problem Solving https://artofproblemsolving.com/.
2. Всероссийский интернет-педсовет http://pedsovet.org/.
3. Единое окно доступа к образовательным ресурсам http://window.edu.ru/.
4. Каталог статей российской образовательной прессы http://periodika.websib.ru/ .

5. Научная электронная библиотека http://elibrary.ru/.
6. Официальный сайт Министерства образования и науки Российской Федерации http://минобрнауки.рф/.
7. Российский общеобразовательный портал http://www.school.edu.ru/.
8. Сообщество взаимопомощи учителей http://pedsovet.su/.
9. Учебно-методический журнал «Математика» издательского дома «Первое сентября» http://mat.1september.ru/ .
10. Федеральный портал «Российское образование» http://www.edu.ru/ .
11. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru/.
12. Федеральный центр информационно-образовательных ресурсов http://fcior.edu.ru/.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

1. Microsoft Office.

9. Технические средства и материально-техническое обеспечение дисциплины

1. Аудитория, оснащенная компьютером и мультимедиа-проектором, для чтения лекций и проведения практических занятий (для всех учебных встреч).

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020г.

ЗАЩИТА ОПЕРАЦИОННЫХ СИСТЕМ
Рабочая программа
для обучающихся по направлению подготовки
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Оленников Е.А. Защита операционных систем. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Защита операционных систем [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Оленников Е.А, 2020.

1. Пояснительная записка

Учебная дисциплина «Защита операционных систем» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Защита операционных систем» является изложение основополагающих принципов защиты операционных систем (ОС) и примеров реализации подобных методов на практике.

Задачи дисциплины «Защита операционных систем»:

- дать представление об основных угрозах для современных ОС;
- научить оценивать уровень защищенности ОС с учетом актуальных моделей угроз и требований руководящих документов;
- дать основы системного подхода к обеспечению безопасности в современных ОС;
- изучить сервисы безопасности современных ОС и научить использовать их для защиты ОС.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Операционные системы», «Администрирование операционных систем».

Дисциплина преподаётся в 7-8 семестре, обеспечиваемых дисциплин нет, вырабатываемые компетенции обеспечивают выполнение выпускной квалификационной работы.

1.2. **Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)**

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОПК-7: способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения		знать: основные понятия программно-технического уровня ИБ; основные сервисы безопасности ОС, принципы их организации и структуру; методы обеспечения ИБ в ОС; уметь: конфигурировать встроенные сервисы безопасности ОС;
ОПК-9: способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации		знать: основные понятия и положения защиты информации в ОС; основные угрозы ИБ в ОС; ресурсы, подлежащие защите; основные понятия программно-технического уровня ИБ; требования к обеспечению ИБ в ОС; основные сервисы безопасности ОС, принципы их организации и структуру;

		методы обеспечения ИБ в ОС; перечень программно-технических мер ИБ в ОС; основные ресурсы для поиска информации об уязвимостях ОС; уметь: проводить анализ угроз информационной безопасности в ОС; проводить классификацию возможных угроз ИБ в ОС; оценивать эффективность и надежность защиты ОС; находить информацию об актуальных угрозах ОС, уязвимостях ОС; выявлять слабые места в защите ОС;
ПК-5: способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической		знать: основные угрозы ИБ в ОС; основные понятия программно-технического уровня ИБ; требования к обеспечению ИБ в ОС; основные сервисы безопасности ОС, принципы их организации и структуру; методы обеспечения ИБ в ОС; уметь: проводить анализ угроз информационной безопасности в ОС; выявлять слабые места в защите ОС; конфигурировать встроенные сервисы безопасности ОС; проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; проводить инструментальный контроль защищенности ОС;
ПК-8: способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы		знать: основные понятия и положения защиты информации в ОС; основные угрозы ИБ в ОС; ресурсы, подлежащие защите; основные понятия программно-технического уровня ИБ; уметь: оценивать эффективность и надежность защиты ОС; находить информацию об актуальных угрозах ОС, уязвимостях ОС;

ПК-15: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы		знать: основные угрозы ИБ в ОС; основные понятия программно-технического уровня ИБ; требования к обеспечению ИБ в ОС; методы обеспечения ИБ в ОС; основные ресурсы для поиска информации об уязвимостях ОС; уметь: проводить анализ угроз информационной безопасности в ОС; проводить классификацию возможных угроз ИБ в ОС; оценивать эффективность и надежность защиты ОС; находить информацию об актуальных угрозах ОС, уязвимостях ОС; выявлять слабые места в защите ОС; проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
ПК-17: способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение		знать: основные сервисы безопасности ОС, принципы их организации и структуру; перечень программно-технических мер ИБ в ОС; уметь: конфигурировать встроенные сервисы безопасности ОС; проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; проводить инструментальный контроль защищенности ОС;
ПК-18: способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем,		знать: основные сервисы безопасности ОС, принципы их организации и структуру; перечень программно-технических мер ИБ в ОС; уметь: конфигурировать встроенные сервисы безопасности ОС;

включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; проводить инструментальный контроль защищенности ОС;
ПСК-3.2: способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем		знать: основные понятия и положения защиты информации в ОС; основные угрозы ИБ в ОС; требования к обеспечению ИБ в ОС; основные сервисы безопасности ОС, принципы их организации и структуру; основные ресурсы для поиска информации об уязвимостях ОС; уметь: проводить анализ угроз информационной безопасности в ОС; эффективность и надежность защиты ОС; находить информацию об актуальных угрозах ОС, уязвимостях ОС; выявлять слабые места в защите ОС; проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; проводить инструментальный контроль защищенности ОС;

* не предусмотрено

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)	
		7 семестр	**8** семестр
Общий объем зач. ед.	**7**	**3.5**	**3.5**
час.	**252**	**126**	**126**
Из них:			
Часы аудиторной работы (всего):	**144**	**72**	**72**
Лекции	72	36	36
Практические занятия		0	0

Лабораторные/практические занятия по подгруппам	72	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	**108**	**54**	**54**
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет	экзамен

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной) и традиционной (5-балльной) систем оценок.

В 7 семестре предусмотрен зачет. Оценка за зачет студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических работ, индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины. Для получения зачета необходимо набрать не менее 61 балла.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «зачет» студент должен сдать минимум 75% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты.

В 8 семестре предусмотрен экзамен. Экзаменационная оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических работ, индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должно быть сдано минимум 50% практических работ и сделан ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен сдать минимум 75% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен сдать минимум 90% практических работ и

ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами.
Примечание. Студент, желающих исправить экзаменационную оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена.4. Содержание дисциплины

4. Содержание дисциплины
4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
Семестр 7						
1.	Основные понятия и положения защиты информации в АС.	8	2	0	2	
2.	Угрозы ИБ: определения, анализ и классификация.	8	2	0	2	
3.	Основные направления и методы реализации угроз ИБ.	12	2	0	4	
4.	Программно-технические меры ИБ, сервисы ИБ.	8	4	0	0	
5.	Требования безопасности информации к операционным системам	8	2	0	2	
6.	Модели безопасности основных операционных систем.	8	2	0	0	
7.	Базовые сервисы безопасности ОС Windows. Реализация, конфигурирование, уязвимости, компрометация, защита.	20	8	0	10	
8.	Дополнительные механизмы защиты в ОС Windows.	8	2	0	2	

9.	Организация защищенного удаленного доступа в ОС Windows.	4	2	0	2	
10.	Сетевая безопасность в ОС Windows.	12	4	0	4	
11.	Аудит безопасности в ОС Windows.	8	2	0	4	
12.	Общие рекомендации по защите ОС Windows.	22	4	0	4	
	Всего (часов) за семестр 7	126	36	0	36	0
Семестр 8						
1.	Базовые сервисы безопасности в Unix-like системах. Реализация, конфигурирование, уязвимости, компрометация, защита.	30	10	0	12	
2.	Дополнительные механизмы защиты объектов ФС в Unix-like системах. Шифрование, контроль целостности.	12	4	0	2	
3.	Мандатная модель управления доступом в Unix-like системах.	16	4	0	4	
4.	Подключаемые модули аутентификации.	10	2	0	2	
5.	Организация защищенного удаленного доступа в Unix-like системах.	8	2	0	2	
6.	Сетевая безопасность в Unix-like системах.	16	4	0	4	
7.	Аудит безопасности в Unix-like системах.	16	4	0	4	
8.	Общие рекомендации по защите ОС	18	6	0	6	
	Всего (часов) за семестр 8	126	36	0	36	2
	Итого (часов)	252	72	0	72	2

4.2. Содержание дисциплины (*модуля*) по темам

Семестр 7.

Основные понятия и положения защиты информации в ИВС.

Информационная безопасность. Защита информации. Безопасная ИС. Предмет и объект защиты информации. Политика ИБ. Разработка защитных мероприятий по обеспечению безопасности ИС. Основные положения безопасности ИС. Основные принципы обеспечения информационной безопасности в АС. Этапы развития концепций обеспечения безопасности данных.

Практическая работа 1.

Подготовка и развёртывание виртуальной инфраструктуры для отработки методов защиты ОС.

Угрозы ИБ: определения, анализ и классификация. Анализ угроз информационной безопасности. Классификация возможных угроз ИБ АС по ряду базовых признаков.

Практическая работа 2.

Использование специализированных источников для получения информации об актуальных угрозах ИБ.

Основные направления и методы реализации угроз ИБ. Структуризация методов обеспечения ИБ. Основные направления реализации угроз информационной безопасности. Классификация злоумышленников.

Практическая работа 3.

Инструментальные средства проверки ОС на наличие уязвимостей.

Программно-технические меры ИБ, сервисы ИБ. Основные понятия программно-технического уровня информационной безопасности. Программно-технические меры ИБ.

Требования безопасности информации к операционным системам.

Обзор нормативной документации.

Модели безопасности основных операционных систем.

Практическая работа 4.

Изучение РД. Подготовка отчета о соответствие ОС требованиям РД.

Базовые сервисы безопасности ОС Windows. Реализация, конфигурирование, уязвимости, компрометация, защита.

Управление локальными и доменными учетными записями. Политики безопасности. Средства контроля доступа. Протоколирование и аудит.

Практическая работа 5.

Изучение способов входа в систему при наличии физического доступа к ЭВМ, изучение и разработка мер противодействия.

Практическая работа 6.

Изучение методов компрометации учетной записи ОС, изучение и разработка мер противодействия.

Практическая работа 7.

Изучение методов эскалации привилегий в ОС Windows, изучение и разработка мер противодействия.

Практическая работа 8.

Компрометация системы контроля доступа, изучение и разработка мер противодействия.

Дополнительные механизмы защиты в ОС Windows.

Практическая работа 9.

Изучение дополнительных механизмов защиты ОС Windows.

Организация защищенного удаленного доступа в ОС Windows.

Практическая работа 10.
Организация защищенного удаленного доступа

Сетевая безопасность в ОС Windows.

Практическая работа 11.
Сетевая безопасность

Аудит безопасности в ОС Windows.

Практическая работа 12.
Аудит безопасности, проведение тестирования на проникновение

Общие рекомендации по защите ОС Windows.
Практическая работа 13.
Реализация комплекса защитных мероприятий на примере собственной виртуальной инфраструктуры.

Семестр 8.

Базовые сервисы безопасности в Unix-like системах. Реализация, конфигурирование, уязвимости, компрометация, защита.
Управление учетными записями. Политики безопасности. Средства контроля доступа. Протоколирование и аудит.
Практическая работа 1.
Подготовка и развёртывание виртуальной инфраструктуры для отработки методов защиты ОС.
Практическая работа 2.
Изучение способов входа в систему при наличии физического доступа к ЭВМ, изучение и разработка мер противодействия.
Практическая работа 3.
Изучение методов компрометации учетной записи ОС, изучение и разработка мер противодействия.
Практическая работа 4.
Компрометация системы контроля доступа, изучение и разработка мер защиты объектов ФС.
Практическая работа 5.
Изучение методов эскалации привилегий в ОС, изучение и разработка мер противодействия.

Дополнительны механизмы защиты объектов ФС в Unix-like системах.
Шифрование, контроль целостности.

Практическая работа 6.
Дополнительны механизмы защиты объектов ФС. Шифрование, контроль целостности.

Мандатная модель управления доступом в Unix-like системах.

Практическая работа 7.
Мандатная модель управления доступом.

Подключаемые модули аутентификации.

Практическая работа 8.
Разработка и применение PAM - модуля

Организация защищенного удаленного доступа в Unix-like системах.

Практическая работа 9.
Организация защищенного удаленного доступа

Сетевая безопасность в Unix-like системах.

Практическая работа 10.
Сетевая безопасность

Аудит безопасности в Unix-like системах.

Практическая работа 11.
Аудит безопасности, проведение тестирования на проникновение

Общие рекомендации по защите ОС.

Практическая работа 12
Реализация комплекса защитных мероприятий на примере собственной виртуальной инфраструктуры.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
Семестр 7		
1.	Основные понятия и положения защиты информации в АС.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
2.	Угрозы ИБ: определения, анализ и классификация.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
3.	Основные направления и методы реализации угроз ИБ.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
4.	Программно-технические меры ИБ, сервисы ИБ.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
5.	Требования безопасности информации к операционным системам	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
6.	Модели безопасности основных операционных систем.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

7.	Базовые сервисы безопасности ОС Windows. Реализация, конфигурирование, уязвимости, компрометация, защита.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
8.	Дополнительные механизмы защиты в ОС Windows.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
9.	Организация защищенного удаленного доступа	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
10.	Сетевая безопасность	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
11.	Аудит безопасности	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
12.	Общие рекомендации по защите ОС Windows.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
Семестр 8		
1.	Общий обзор Unix-like систем. ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
2.	Командная строка FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
3.	Управление локальными пользователями в ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
4.	Управление дисковыми ресурсами, ФС UFS.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
5.	Ограничение доступа к файлам и каталогам.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
6.	Сетевые параметры в ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
7.	Загрузка ОС FreeBSD. Сборка ядра, обновление системы.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
8.	Установка программного обеспечения в ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
9.	Сервер имен под управлением ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
10.	DHCP-сервера под управлением ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
11.	Файловый сервер под управлением ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
12.	Организация удаленного доступа к серверу под управлением ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
13.	Организация резервного копирования и восстановления данных в ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
14.	Мониторинг работы и контроль	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

	производительности ОС FreeBSD.	
15.	Обеспечение отказоустойчивости ОС FreeBSD.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение основной и дополнительной литературы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации – зачет (7 семестр), экзамен (8 семестр). Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса.

Вопросы к зачету.

7 семестр

1. Определение понятий: информационная безопасность, защита информации, конфиденциальность, доступность, целостность.
2. Свойства информации: ценность, достоверность, своевременность.
3. Предмет защиты информации. Объект защиты информации. Информационная безопасность АСОИ. Политика информационной безопасности. Система защиты информации.
4. Основные положения безопасности информационных систем. Основные принципы обеспечения информационной безопасности в информационных системах.
5. Определение понятий: угроза, угроза информационной безопасности АС, атака, злоумышленник, источник угрозы, уязвимость, окно опасности,
6. Классификация возможных угроз ИБ АС по ряду базовых признаков.
7. Угроза доступности. Угроза нарушения целостности. Угроза нарушения конфиденциальности.
8. Уровни доступа к информации.
9. Классификация злоумышленников.
10. Основные направления реализации угроз информационной безопасности.
11. Программно-технические меры ИБ.
12. Основные и вспомогательные сервисы безопасности.
13. Идентификация и аутентификация.
14. Классификация требований к системам защиты.
15. Формализованные требования к защите компьютерной информации АС.
16. Механизмы защиты операционных систем. Типовые функциональные дефекты ОС, приводящие к созданию каналов утечки данных.
17. Контроль доступа к данным в ОС. Субъекты и объекты доступа. Полномочия. Логическое управление доступом.
18. Дискреционные модели доступа. Модели безопасности на основе мандатной политики.
19. Принципиальные недостатки защитных механизмов ОС семейства Windows, Unix.
20. Система безопасности операционной системы Windows. SAM.

21. Система безопасности операционной системы Windows. Идентификаторы защиты. Маркеры доступа. Дескрипторы защиты и управление доступом.
22. Управление пользователями в ОС Windows. Децентрализованная (Рабочие группы) и централизованная (домены) модель управления. Групповая политика безопасности.
23. Методы компрометации учетной записи пользователя в Windows и методы противодействия компрометации учетной записи.
24. Методы эскалации привилегий в ОС Windows, меры противодействия.
25. Файловая система NTFS: контроль доступа к объектам файловой системы, квотирование, шифрование (EFS).
26. Методы компрометации системы контроля доступа, меры противодействия.
27. Дополнительные механизмы защиты ОС Windows.
28. Методы инструментального контроля уровня защищенности ОС.
29. Общие рекомендации по защите ОС Windows.

Вопросы к экзамену.

8 семестр

1. Базовые сервисы безопасности в Unix-like системах.
2. Типовые уязвимости Unix-like систем.
3. Примеры уязвимостей сервисов безопасности в Unix-like системах и меры противодействия (на примере одного из сервисов).
4. Базовые методы управление пользователями в Unix-like системах.
5. Методы компрометации учетной записи пользователя в Unix-like системах и методы противодействия.
6. Методы ограничения пользователей в Unix-like системах.
7. Методы повышения привилегий. Выполнение команд от имени других пользователей. Утилиты su, sudo.
8. Базовые методы контроля доступа к объектам ФС в Unix-like системах.
9. Расширенные средства контроля доступа к объектам ФС в Unix-like системах: специальные флаги, ACL.
10. Методы компрометации системы контроля доступа, меры противодействия в Unix-like системах (примеры).
11. Шифрование объектов ФС в Unix-like системах.
12. Реализация контроля целостности объектов ФС в Unix-like системах.
13. Мандатная модель управления доступом в Unix-like системах.
14. Сетевая безопасность в Unix-like системах. Общие положения.
15. Межсетевые экраны в Unix-like системах. Принцип работы, пример конфигурирования.
16. Системы аудита и службы системной журнализации. Общие принципы работы и конфигурирования.
17. Организация защищенного удаленного доступа в Unix-like системах.
18. Аудит безопасности в Unix-like системах. Общие принципы использования, используемые средства.
19. Подключаемые модули аутентификации (PAM). Общее описание, пример использования.
20. Принудительный контроль доступа (MAC). Описание политик, пример настройки.

Общие подходы к защите современных ОС.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОПК-7: способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	**Знает**: основные понятия программно-технического уровня ИБ; основные сервисы безопасности ОС, принципы их организации и структуру; методы обеспечения ИБ в ОС; **Умеет**: конфигурировать встроенные сервисы безопасности ОС;	Практическая работа. Зачет. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ОПК-9: способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	**Знает**: основные понятия и положения защиты информации в ОС; основные угрозы ИБ в ОС; ресурсы, подлежащие защите; основные понятия программно-технического уровня ИБ; требования к обеспечению ИБ в ОС; основные сервисы безопасности ОС, принципы их организации и структуру; методы обеспечения ИБ в ОС; перечень программно-технических мер ИБ в ОС;	Практическая работа. Зачет. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно

		основные ресурсы для поиска информации об уязвимостях ОС; **Умеет**: проводить анализ угроз информационной безопасности в ОС; проводить классификацию возможных угроз ИБ в ОС; оценивать эффективность и надежность защиты ОС; находить информацию об актуальных угрозах ОС, уязвимостях ОС; выявлять слабые места в защите ОС;		требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
3.	ПК-5: способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической	**Знает**: основные угрозы ИБ в ОС; основные понятия программно-технического уровня ИБ; требования к обеспечению ИБ в ОС; основные сервисы безопасности ОС, принципы их организации и структуру; методы обеспечения ИБ в ОС; **Умеет**: проводить анализ угроз информационной безопасности в ОС; выявлять слабые места в защите ОС; конфигурировать встроенные сервисы безопасности ОС; проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; проводить инструментальный контроль защищенности ОС;	Практическая работа. Зачет. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
4.	ПК-8: способностью участвовать в разработке подсистемы информационной	**Знает**: основные понятия и положения защиты информации в ОС; основные угрозы ИБ в ОС;	Практическая работа. Зачет. Экзамен.	Компетенция сформирована при правильности и полноте ответов на

	безопасности компьютерной системы	ресурсы, подлежащие защите; основные понятия программно-технического уровня ИБ; **Умеет**: оценивать эффективность и надежность защиты ОС; находить информацию об актуальных угрозах ОС, уязвимостях ОС;		теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
5.	ПК-15: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	**Знает**: основные угрозы ИБ в ОС; основные понятия программно-технического уровня ИБ; требования к обеспечению ИБ в ОС; методы обеспечения ИБ в ОС; основные ресурсы для поиска информации об уязвимостях ОС; **Умеет**: проводить анализ угроз информационной безопасности в ОС; проводить классификацию возможных угроз ИБ в ОС; оценивать эффективность и надежность защиты ОС; находить информацию об актуальных угрозах ОС, уязвимостях ОС; выявлять слабые места в защите ОС; проводить проверку работоспособности и эффективности применяемых программных, программно-	Практическая работа. Зачет. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся

		аппаратных и технических средств защиты информации;		ФГАОУ ВО ТюмГУ»
6.	ПК-17: способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение	**Знает**: основные сервисы безопасности ОС, принципы их организации и структуру; перечень программно-технических мер ИБ в ОС; **Умеет**: конфигурировать встроенные сервисы безопасности ОС; проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; проводить инструментальный контроль защищенности ОС;	Практическая работа. Зачет. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
7.	ПК-18: способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные	**Знает**: основные сервисы безопасности ОС, принципы их организации и структуру; перечень программно-технических мер ИБ в ОС; **Умеет**: конфигурировать встроенные сервисы безопасности ОС; проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; проводить инструментальный контроль защищенности ОС;	Практическая работа. Зачет. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о

	сети, системы антивирусной защиты, средства криптографической защиты информации			текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
8.	ПСК-3.2: способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем	**Знает**: основные понятия и положения защиты информации в ОС; основные угрозы ИБ в ОС; требования к обеспечению ИБ в ОС; основные сервисы безопасности ОС, принципы их организации и структуру; основные ресурсы для поиска информации об уязвимостях ОС; **Умеет**: проводить анализ угроз информационной безопасности в ОС; эффективность и надежность защиты ОС; находить информацию об актуальных угрозах ОС, уязвимостях ОС; выявлять слабые места в защите ОС; проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; проводить инструментальный контроль защищенности ОС;	Практическая работа. Зачет. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Безопасность сетей : учебное пособие. — 2-е изд. — Москва : ИНТУИТ, 2016. — 571 с. — ISBN 5-9570-0046-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100581 (дата обращения: 15.05.2020)

7.2. Дополнительная литература:

1. Джонс, К. Д. Инструментальные средства обеспечения безопасности : учебное пособие / К. Д. Джонс, М. Шема, Б. С. Джонсон. — 2-е изд. — Москва : ИНТУИТ, 2016. — 914 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100602 (дата обращения: 15.05.2020).

2. Нестеров, С. А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft : учебное пособие / С. А. Нестеров. — 2-е изд. — Москва : ИНТУИТ, 2016. — 250 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100566 (дата обращения: 15.05.2020).

7.3. Интернет-ресурсы

1. вузовские электронно-библиотечные системы учебной литературы.
2. доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru.
3. https://fstec.ru/
4. https://www.cvedetails.com/

7.4 Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) https://icdlib.nspu.ru/
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА https://rusneb.ru/
- Справочная правовая система КонсультантПлюс http://www.consultant.ru/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Программное обеспечение виртуализации: VMWare, VirtualBox или другое.
- Операционная система Windows 7 или более поздние версии.
- Операционная система Windows Server 2012 или более поздние версии.
- Операционная система Linux, Unix-like система.
- Офисный пакет.
- Платформа для электронного обучения Microsoft Teams.

9. **Технические средства и материально-техническое обеспечение дисциплины (модуля)**

Лекционная аудитория с проектором. Компьютерный класс с установленным ПО.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020г.

ЗАЩИТА ПРОГРАММ И ДАННЫХ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Шабалин А.М. Защита программ и данных. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.
Рабочая программа дисциплины опубликована на сайте ТюмГУ: Защита программ и данных [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Шабалин А.М, 2020.

1. Пояснительная записка

Защита программ и данных обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Цель дисциплины «Защита программ и данных» является изучение программных способов и методов защиты современных сетевых сервисов и протоколов маршрутизации, а также - изучение основных подходов к эксплуатации технологий защиты при передаче информации в сети предприятия.

Задачи курса:

• Анализ принципов функционирования и защиты современных протоколов маршрутизации в сети предприятия;

• Организация безопасных базовых сервисов в сети предприятия средствами современного телекоммуникационного оборудования;

• Изучение функциональных возможностей современных технологий защиты передачи информации в сети предприятия.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Языки программирования», «Технологии и методы программирования», «Разработка и защита web-приложений».

Дисциплина «Защита программ и данных» способствует освоению преддипломной практики, защиты выпускной квалификационной работы (дипломная работа).

.

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОПК-8 - способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач		знает Угрозы нарушения информационной безопасности компьютерных сетей Основные криптографические методы защиты информации Архитектуру и функции систем управления сетями, стандарты систем управления Принципы функционирования защищенных сетевых протоколов Средства мониторинга и анализа компьютерных сетей Методы устранения неисправностей в технических системах умеет Применять основные протоколы и технологии обеспечения безопасности компьютерных сетей Выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств Осуществлять диагностику и поиск неисправностей всех компонентов сети Выполнять действия по устранению неисправностей

* не предусмотрено

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	Всего часов (академические часы)	Часов в семестре (академические часы)
		9 семестр
Общий объем зач. ед.	4	4
час.	144	144
Из них:		
Часы аудиторной работы (всего):	72	72
Лекции	36	36
Лабораторные занятия		
Практические занятия по подгруппам	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	72	72
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		экзамен

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной) и традиционной (4-балльной) систем оценок.

Экзаменационная оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время лабораторных работ, индивидуальных домашних заданий, контрольной работы. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:
61 - 76 баллов - удовлетворительно;
77 - 90 баллов - хорошо;
91 -100 баллов - отлично.
Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать экзамен.

Экзаменационная оценка студента в рамках традиционной системы оценок выставляется на основе ответа студента на теоретические вопросы, а также выполнения заданий, примерный уровень которых соответствует уровню заданий, выполняемых в семестре при проведении контрольных работ. Эта оценка характеризует уровень знаний, умений и навыков, приобретенных студентом в ходе изучения дисциплины.
Примечание. Студент, желающих исправить экзаменационную оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена.
Каждая лекция оценивается в 1 балл (посещение, конспектирование материала, работа на лекции). Каждое практическое/семинарское/лабораторное занятие выполняется предложенная работа по теме лекции, которая оценивается в зависимости от сложности задания.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№	Наименование тем и/или разделов	Объем дисциплины (модуля), час				
		Всего	Виды аудиторной работы (в час)			Иные виды контактной работы
			Лекции	Практические занятия по подгруппам	Лабораторные занятия	
1	2	3	4	5	6	7
1.	Защита программ и данных в компьютерной сети.		4	4	0	0
2.	Маршрутизация в сети предприятия.		4	4	0	0
3.	Статические маршруты для IPv4 / IPv6		4	4	0	0
4.	Защита протокола RIP.		4	4	0	0
5.	Защита протокола EIGRP.		4	4	0	0
6.	Защита протокола OSPF.		4	4	0	0
7.	Подключение сети предприятия к сети Интернет с использованием протокола BGP.		4	4	0	0
8.	Защита основных сервисов сети предприятия		4	4	0	0
9.	Защита передаваемых по сети данных.		4	4	0	0
	Итого (часов)	144	36	36	0	2

4.2. Содержание дисциплины (*модуля*) по темам

1. Защита программ и данных в компьютерной сети.
Дизайн сети предприятия. Особенности сетевых приложений. Канальные среды.
2. Маршрутизация в Cisco IOS. CEF. Механизмы манипуляции маршрутной информацией. Policy Base Routing.
3. Статические маршруты для IPv4 / IPv6.
Особенности использования. Виды статических маршрутов. Варианты применения.
4. Защита протокола RIP.
Базовый функционал безопасной работы протоколов динамической маршрутизации. Особенности работы протокола RIPv2.
5. Защита протокола EIGRP.
EIGRP RTP. Манипуляции с маршрутами в EIGRP. Расширенный функционал аутентификации в EIGRP Named Mode.
6. Защита протокола OSPF.
Типы LSA в OSPFv2. OSPFv2 LSDB. Манипуляции с маршрутами в OSPFv2.
Шифрование маршрутной информации IPSEC в протоколе OSPFv3.
7. Подключение сети предприятия к сети Интернет с использованием протокола BGP.
Безопасность сети предприятия в стыках с сетью Интернет. Атрибуты BGP. BGP AF-Mode.
8. Защита основных сервисов сети предприятия.

Протоколы динамической конфигурации хоста DHCPv4 / DHCPv6. Служба доменных имен DNS. Протокол удаленного управления SSH.

9. Защита передаваемых по сети данных.

Простой протокол передачи файлов TFTP. Аутентификация и авторизация в протоколе FTP. Шифрование трафика протоколом SCP.

Планы практических занятий

Практическая работа № 1-2. Настройка канальных среды в Cisco IOS / Huawei VRP.

Конфигурирование протоколов HDLC, PPP, Frame Relay. Особенности построения туннелей GRE и DMVPN.

Практическая работа № 3-4. Policy Base Routing в Cisco IOS / Huawei VRP.

Конфигурирование access-list, prefix-list, distribute-list, route-map.

Практическая работа № 5-6. Static Routing в Cisco IOS / Huawei VRP.

Конфигурирование маршрутов по умолчанию, суммарных и плавающих статических маршрутов.

Практическая работа № 7-8. RIP в Cisco IOS / Huawei VRP.

Конфигурирование ключевых цепочек и аутентификации. Определение пассивных интерфейсов и включение запрета на получения update-сообщений.

Практическая работа № 9-10. EIGRP в Cisco IOS.

Конфигурация безопасной работы протокола EIGRP в классическом (Classic Mode) и именованном режимах (Named Mode).

Практическая работа № 11-12. OSPFv2 / OSPFv3 в Cisco IOS / Huawei VRP.

Конфигурация безопасной работы протокола OSPF в режимах: OSPFv2 / OSPFv3 Classic Mode и OSPFv3 AF-mode.

Практическая работа № 13-14. BGP в Cisco IOS. Работа с атрибутами BGP в Cisco IOS / Huawei VRP.

Конфигурирование BGP. Работа с атрибутами BGP. Настройка BGP AF-Mode.

Практическая работа № 15-16. DHCPv4 / DHCPv6, DNS, SSH в Cisco IOS / Huawei VRP.

Конфигурирование и защита DHCPv4. Настройка автоконфигурации хостов с технологией SLAAC и DHCPv6 с отслеживанием состояния и без отслеживания состояния. Конфигурирование DNS-сервера на маршрутизаторах. Тонкие настройки безопасного подключения по SSH.

Практическая работа № 17-18. TFTP. FTP. SCP в Cisco IOS / Huawei VRP.

Конфигурирование TFTP, FTP, SCP-серверов на коммуникационном оборудовании. Безопасное резервирование настроек и обновление операционных систем коммуникационных устройств.

Образцы средств для проведения текущего контроля

Проверка качества подготовки в течение семестра предполагает следующие виды промежуточного контроля:

А) модели сети на Packet Tracer;

Б) выполнение расчетной работы на компьютере в группах;

Примерные темы расчетных работ - моделей сети для Packet Tracer:

- Защита программ и данных в компьютерной сети.
- Маршрутизация в сети предприятия.
- Статические маршруты для IPv4 / IPv6
- Защита протокола RIP.

- Защита протокола EIGRP.
- Защита протокола OSPF.
- Подключение сети предприятия к сети Интернет с использованием протокола BGP.
- Защита основных сервисов сети предприятия
- Защита передаваемых по сети данных.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Защита программ и данных в компьютерной сети.	Чтение обязательной литературы, подготовка к практическим занятиям
2.	Маршрутизация в сети предприятия.	Чтение обязательной литературы, подготовка к практическим занятиям
3.	Статические маршруты для IPv4 / IPv6	Чтение обязательной литературы, подготовка к практическим занятиям
4.	Защита протокола RIP.	Чтение обязательной литературы, подготовка к практическим занятиям
5.	Защита протокола EIGRP.	Чтение обязательной литературы, подготовка к практическим занятиям
6.	Защита протокола OSPF.	Чтение обязательной литературы, подготовка к практическим занятиям
7.	Подключение сети предприятия к сети Интернет с использованием протокола BGP.	Чтение обязательной литературы, подготовка к практическим занятиям
8.	Защита основных сервисов сети предприятия	Чтение обязательной литературы, подготовка к практическим занятиям
9.	Защита передаваемых по сети данных.	Чтение обязательной литературы, подготовка к практическим занятиям

Порядок выполнения каждого вида самостоятельной работы:
1. Изучение лекционного материала по теме.
2. Изучение рекомендованной основной и дополнительной литературы.
3. Разбор примеров практических работ.

Контроль за самостоятельной работой осуществляется при выполнении обучающимся теста, контрольной работы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. **Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)**

Форма проведения промежуточной аттестации – экзамен. Экзамен проводится в виде контрольной работы.

Пример задания: Экзаменационный билет содержит 2 вопроса из списка примерных вопросов и 1 практического задания.

Теоретическая часть:

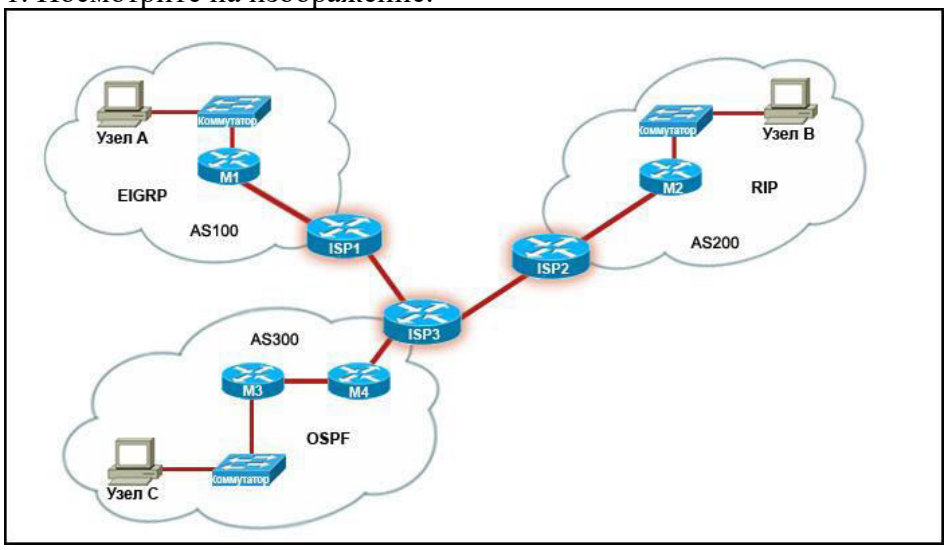
Вопросы к экзамену.

1. Назначение и виды протоколов динамической маршрутизации. Сетевая инфраструктура предприятия.
2. Задачи протоколов динамической маршрутизации и их роль в сети предприятия. Выбор протокола динамической маршрутизации.
3. Типы протоколов динамической маршрутизации. Понятие сходимости. Суммаризация маршрутов. Масштабируемость протоколов динамической маршрутизации.
4. Типы сетевого трафика. Типы IPv6-адресов. Типы сетевых топологий (point-to-point, broadcast, NBMA, point-to-multipoint).
5. Маршрутизация в Интернет. Задача организации связи между частями сети предприятия — выбор технологий.
6. Маршрутизация при сформированных GRE-туннелях.
7. DMVPN (Dynamic Multipoint Virtual Private Network) и использование mGRE / NHRP. IPsec как метод обеспечения безопасности для DMVPN.
8. Простой протокол динамической маршрутизации — RIP (RIPng / RIPv2).
9. Основные особенности протокола EIGRP. Обеспечение надёжности распространения маршрутной информации.
10. Основные алгоритмы работы EIGRP. Таймеры EIGRP.
11. Топология EIGRP-роутеров: обмен маршрутной информацией. Метрика, используемая EIGRP. Формула метрики, пример расчёта метрики. Feasibility Condition.
12. Оптимизация работы EIGRP. Схема Query-Reply. Зачем нужны EIGRP Stub Router'ы. Состояние Stuck in Active и работа SIA-Query / SIA-Reply. Суммаризация маршрутов в EIGRP. Балансировка трафика с использованием EIGRP.
13. EIGRP для IPv6 — настройка и управление. Работа Named EIGRP и новый вариант настройки EIGRP — через именованные контексты.
14. Основные особенности протокола OSPF. Работа протокола OSPF. Иерархическая структура и разбиение сети на регионы (area) в OSPF. Технические ограничения протокола OSPF.
15. Типы пакетов в OSPF. Типы сетей, определяемые OSPF и особенности работы протокола.
16. Фазы взаимодействия OSPF-роутеров друг с другом. Использование passive interface.
17. Работа LSDB и типы LSA. Как LSDB работает, синхронизируется и делает фоновые операции. Алгоритм SPF. Подсчёт стоимости маршрутов в простом случае (внутри региона) и сложном (между регионами).
18. Суммаризация маршрутов в OSPF. Разные типы суммаризации OSPF — для ABR и ASBR-роутеров. Маршрут по-умолчанию в OSPF.
19. Работа OSPFv3 — обычного (для IPv6) и обновлённого (IPv4 / IPv6).
20. Обмен маршрутами (редистрибьюция). Задачи обмена маршрутами и типовые алгоритмы (формирование метрики по-умолчанию).
21. Специфика подсчёта стоимости для E1 и E2-маршрутов в OSPF при редистрибьюции. Односторонняя и взаимная редистрибьюция.
22. Работа distribute lists и prefix lists. Фильтрация при редистрибьюции маршрутов, поступающих от другого источника.
23. Работа route map. Эффективное применение и оптимизация использования route map как для фильтрации, так и для модификации параметров маршрутов. Метки маршрутов — route tags. Изменение приоритета (administrative distance) у маршрутов.
24. Общая логика Path Control. Понятие Control Plane и Data Plane.
25. Механизмы L3-коммутации. Process Switching и Fast Switching. Механизм Cisco Express Forwarding.
26. Задачи Path Control. PBR (policy-based routing) — преимущества и основные варианты использования. Настройка PBR.
27. Работа Dynamic Path Control. Пример использования механизма Cisco IOS IP SLA.

28. Задачи, решаемые при подключении сети предприятия к Интернет.
29. Типы и варианты подключения к провайдеру. Назначение IP-адресов и автономных систем (AS).
30. Простое подключение с использованием диапазон IPv4-адресов.
31. Работа NAT. Статический и динамический NAT. PAT. Настройка виртуальных интерфейсов для NAT.
32. Подключение к провайдеру по IPv6-префиксу. Основы безопасности внешнего IPv6-подключения.
33. Проблемы одного подключения к Интернет. Подключение к нескольким провайдерам и настройка маршрутов трафика для оптимального использования всех преимуществ нескольких подключений.
34. Преимущества использования BGP в сценарии работы с несколькими провайдерами.
35. Работа протоколов семейства Path Vector. Политики для управления маршрутами BGP. Как работает BGP и как устанавливаются peer-отношения между BGP-маршрутизаторами.
36. Различия во взаимодействии у EBGP и IBGP-соседей.
37. Механизм и логика выбора лучшего пути в протоколе BGP. Атрибут Weight. Атрибут MED (Multi-exit discriminator). Управление атрибутами BGP, используя route map.
38. Фильтрация получаемой и отправляемой BGP-информации — используя prefix list, AS path access list, route map. Оптимизация работы BGP, используя peer group.
39. Работа MP-BGP — сразу с несколькими протоколами сетевого уровня (IPv4 + IPv6). Обмен IPv6-маршрутами через BGP. Dual Transport и фильтрация получаемой маршрутной информации. Использование атрибута Local Preference для выбора маршрута для IPv6-трафика.
40. Ключевые задачи обеспечения безопасности маршрутизаторов.
41. Шифрование паролей. Использование SSH. Использование ACL для ограничения возможностей доступа к management plane маршрутизатора. Безопасное использование SNMP.
42. Резервное копирование конфигурации маршрутизатора. Журналирование действий. Отключение неиспользуемых служб.
43. Использование аутентификации при работе протоколов динамической маршрутизации. Типы аутентификации. Ротация ключевой информации.
44. Настройка аутентификации для протоколов EIGRP, OSPF, BGP.
45. Настройка DHCP на коммутаторе. DHCP Relay. Настройка DHCPv6. Специфика stateless-режима DHCPv6.

Примеры практических заданий

1. Посмотрите на изображение.



Какой метод чаще всего используется крупными поставщиками услуг Интернета, такими как ISP1, ISP2 и ISP3, для обработки данных маршрутизации и обмена ими?

- статические маршруты
- протоколы IGP
- протоколы EGP+
- маршруты с прямым подключением

2. Какая характеристика является характеристикой протокола маршрутизации EIGRP?

- Он имеет ограничение на число переходов, которое делает протокол пригодным только для сетей, включающих менее 15 переходов.
- Обновления маршрутизации этого протокола не включают маску подсети.
- Он строит таблицу топологии на основе всех объявлений от соседних устройств.+
- Он ведет полную базу данных удаленных маршрутизаторов и методов их соединения.

3. При поиске и устранении неполадок подключения к WAN между главным офисом и офисами филиалов клиента специалист поставщика услуг Интернета проверяет конфигурацию маршрутизатора, чтобы убедиться, что она не была изменена (относительно исходной) сетевым администратором клиента. Какой тип оборудования представляет маршрутизатор?

- CPE+
- POP
- IXP
- устройство CSU/DSU

4. Посмотрите на изображение.

```
RTA# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    10.0.0.0/8 [120/2] via 192.168.1.226, 00:00:17, Serial0/0/0
     192.168.1.0/26 is subnetted, 2 subnets
C       192.168.1.64 is directly connected, FastEthernet0/0
C       192.168.1.192 is directly connected, Serial0/0/0
R    192.168.2.0/24 [120/1] via 192.168.1.226, 00:00:17, Serial0/0/0
R    192.168.3.0/24 [120/1] via 192.168.1.226, 00:00:17, Serial0/0/0
RTA#
```

Укажите часть таблицы маршрутизации, в которой задается вектор в алгоритме маршрутизации на базе вектора расстояния.

- административное расстояние
- шлюз "последней надежды"
- IP-адрес следующего перехода+
- количество переходов

Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОПК-8 - способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	знает Угрозы нарушения информационной безопасности компьютерных сетей Основные криптографические методы защиты информации Архитектуру и функции систем управления сетями, стандарты систем управления Принципы функционирования защищенных сетевых протоколов Средства мониторинга и анализа компьютерных сетей Методы устранения неисправностей в технических системах умеет Применять основные протоколы и технологии обеспечения безопасности компьютерных сетей Выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи - Задание для экзамена в виде контрольной работы	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

		Осуществлять диагностику и поиск неисправностей всех компонентов сети Выполнять действия по устранению неисправностей		

* - не предусмотрен

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 368 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100522 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

7.2. Дополнительная литература:

1. Кияев, В. И. Безопасность информационных систем : учебное пособие / В. И. Кияев, О. Н. Граничин. — 2-е изд. — Москва : ИНТУИТ, 2016. — 191 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100580 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.
2. Олифер, В. Г. Основы сетей передачи данных : учебное пособие / В. Г. Олифер, Н. А. Олифер. — 2-е изд. — Москва : ИНТУИТ, 2016. — 219 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100346 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.
3. Построение коммутируемых компьютерных сетей : учебное пособие / Е. В. Смирнова, И. В. Баскаков, А. В. Пролетарский, Р. А. Федотов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 428 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100370 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

7.3. Интернет-ресурсы

1. Интернет ресурсы Academy Cisco http://netacad.com

7.4 Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) https://icdlib.nspu.ru/
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА https://rusneb.ru/
- Справочная правовая система КонсультантПлюс http://www.consultant.ru/

Наименование ПО

- Microsoft Office 365
- "Microsoft Imagine Academy (ранее Dreamspark):MS Visual Studio, MS SQL Server,ОС семейства MS Windows,MS Visio, MS Project"

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

эмулятор сетей PacketTracer.версия 7.x;

эмулятор сетей GNS3 2.*
эмулятор сетей eNSP 1.3.*
гипервизор Oracle Virtual Box 5.*
платформа для электронного обучения Microsoft Teams
Интернет, доступ в информационно-образовательную среду ТюмГУ, включающую в себя доступ к учебным планам и рабочим программам, к изданиям электронной библиотечной системы.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Компьютерный класс с выходом в интернет и стандартное лабораторное и периферийное оборудование классом не ниже чем в приведенной ниже конфигурации.

- 3 маршрутизатора Cisco 2801 с Base IP IOS, 128 Мбайт DRAM, 32 Мбайта флэш-памяти и модулями HWIC-2A/S;
- 3 коммутатора Cisco Catalyst 2960;
- Набор последовательных кабелей и витой пары;
- 2 беспроводных маршрутизатора Linksys (предпочтительно Linksys WRT150N; допустимо использование моделей WRT54G, WRT300N и WRT350N) или аналогичные устройства SOHO;

Для проведения лекционных и практических занятий необходим проектор с разрешением не менее 800x1200 подключенный к компьютеру с выходом в Интернет.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020г.

ИНТЕРНЕТ ВЕЩЕЙ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Широких А.В. Интернет вещей. Рабочая программа для обучающихся по направлению подготовки 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Интернет вещей [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Широких А.В., 2020.

1. Пояснительная записка

Цели и задачи дисциплины

Цель дисциплины: сформировать навыки разработки и анализа проектов интернета вещей при решении разнообразных прикладных задач.

Задачи дисциплины:

- сформировать понимание принципов разработки и функционирования сенсоров и установок IoT;
- развить навыки использования сенсоров IoT и разработки устройств IOT.

1.1. Место дисциплины в структуре основной образовательной программы.

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. В соответствии с учебным планом образовательной программы изучение данной дисциплины предусмотрено в 6 семестре.

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (модуля)

Код и наименование компетенции	Код и наименование части компетенции*	Планируемые результаты обучения (знаниевые/функциональные)
ОПК-7 - способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения		Знает: архитектуру устройств ИВ и особенности сенсоров ИВ. Умеет: разрабатывать устройства ИВ с учётом особенностей сенсоров ИВ и их взаимодействия с современными системами ИВ.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		6 семестр
Общий объем зач. ед.	**3**	**3**
час.	**108**	**108**
Из них:		
Часы аудиторной работы (всего):	**72**	**72**
Лекции	36	36
Практические занятия		
Лабораторные/практические занятия по подгруппам	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	**36**	**36**

Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной) и традиционной (5-балльной) систем оценок.

В 6 семестре предусмотрен зачет. Оценка за зачет студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических работ, индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины. Для получения зачета необходимо набрать не менее 61 балла.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «зачет» студент должен сдать минимум 75% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы, её взаимосвязь с другими разделами и дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	**Наименование тем и/или разделов**	**Объем дисциплины (модуля), час.**				
		Всего	**Виды аудиторной работы** (академические часы)			**Иные виды контактной работы**
			Лекции	**Практические занятия**	**Лабораторные /практические занятия по подгруппам**	
1	2	3	4	5	6	7
Семестр 6						
1	Введение в дисциплину	17	4		4	
2	Аналоговые сенсоры	29	10		10	
3	Сети IoT. Устройства и цифровые сенсоры.	35	13		13	
4	Взаимодействие с Интернет	27	9		9	
	Всего (часов) за семестр 6	108	36		36	
Семестр						
	Всего (часов) за семестр					
	Итого (часов)	108	36		36	

4.2. Содержание дисциплины *(модуля)* по темам

Семестр 6

Введение в дисциплину

Основные цели и задачи изучения дисциплины. Структура курса. Организация лекционных и практических занятий. Самостоятельная работа. Формы контроля. Основные понятия IoT: микроконтроллеры, сенсоры, исполнительные устройства, сети. Разработка проектов на базе Arduino и его клонов

Практическая работа

Регистрация в системе Tinkercad

Сборка простейшей цепи в Tinkercad

Практическая работа

Разработка кнопочного выключателя

Практическая работа

Разработка проходного кнопочного выключателя

Практическая работа

Разработка проходного кнопочного выключателя без использования микроконтроллера

Аналоговые сенсоры

Сенсоры с аналоговым сигналом. Протокол. Программирование. Преимущества и недостатки аналогового сигнала. Аналоговые сенсоры температуры, давления, расстояния, анемометры, влажности почвы, освещенности, линии, цвета, звука, шума и другие. Примеры проектов с аналоговыми датчиками. Делитель напряжения. Реле и их разновидности. Использование реле для управления мощными потребителями. Разработка устройства для измерения сопротивления.

Практическая работа

Разработка аналогового омметра. Калибровка.

Практическая работа

Разработка аналогового термометра. Калибровка.

Практическая работа

Разработка устройства «контроль влажности почвы» с аналоговым датчиком влажности почвы.

Практическая работа

Разработка устройства «управляемый электронагреватель» с аналоговым термодатчиком.

Практическая работа

Разработка устройства «умное освещение» с аналоговым датчиком освещения.

Сети IoT. Устройства и цифровые сенсоры.

Сеть I2C. Протокол. LCD1602: возможности и подключение по I2C к Ардуино. EEPROM: возможности и подключение по I2C. Датчик температуры I2C MCP9808. Другие I2C сенсоры и устройства. Сети 1-Wire. Протокол. Термодатчик DS18B20 и его разновидности. Устройства IButton. Протокол передачи данных SPI. Сети RS-232, RS-485. Протоколы Modbus. Модули геопозиционирования.

Практическая работа

Разработка цифрового термометра на базе датчика температуры MCP9808 и дисплея LCD1602.

Практическая работа

Хранение и изменения настроек устройств IoT с использованием EEPROM.

Практическая работа

Разработка цифрового термометра на базе датчика температуры DS18B20 и дисплея LCD1602.

Практическая работа

Разработка устройства мониторинга температуры в нескольких помещениях на базе датчиков температуры DS18B20 подключенных к одной линии и дисплея LCD1602.

Практическая работа

Разработка СКУД с использованием устройств IButton.

Практическая работа

Разработка настольных часов на базе RTC (DS1302, DS1307, DS3231) и LCD1602.

Практическая работа

Разработка будильника с использованием RTC (DS1302, DS1307, DS3231), EEPROM, LCD1602.

Практическая работа

Разработка устройства мониторинга температуры в нескольких помещениях на базе датчиков температуры DS18B20 подключенных к одной линии с обработкой данных на ПК (с использованием серийного подключения).

Взаимодействие с Интернет

Протоколы HTTP. Разработка простого HTTP сервера. Работа с проводным интернет. Модули WiFi. GSM модемы.

Практическая работа

Разработка устройства мониторинга температуры в нескольких помещениях на базе датчиков температуры DS18B20 подключенных к одной линии с передачей данных по проводному Интернет на веб сервер.

Практическая работа

Разработка устройства мониторинга температуры в нескольких помещениях на базе датчиков температуры DS18B20 подключенных к одной линии с передачей данных на веб сервер по сети WiFi.

Практическая работа

Разработка устройства мониторинга температуры в нескольких помещениях на базе устройств WEMOS, датчиков температуры DS18B20 подключенных к одной линии с передачей данных по проводному Интернет на веб сервер.

Практическая работа

Разработка устройства мониторинга температуры в нескольких помещениях на базе устройств WEMOS, датчиков температуры DS18B20 подключенных к одной линии с передачей данных по проводному Интернет через GSM модем.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1	Введение в дисциплину	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
2	Аналоговые сенсоры	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
3	Сети IoT. Устройства и цифровые сенсоры.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
4	Взаимодействие с Интернет	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение основной и дополнительной литературы.
3. Разбор примеров практических занятий.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации – зачет (6 семестр) . Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса.

Вопросы к зачету

6 семестр

1. Понятия микроконтроллера, сенсоров и исполнительных устройств, их назначение и примеры
2. Разработка сложных устройств IoT без использования микроконтроллера.
3. Аналоговые сенсоры. Преимущества и недостатки. Калибровка. Примеры аналоговых сенсоров.
4. Использование аналогового датчика давления. Подключение, программное чтения значений давления. Преимущества и недостатки других датчиков.
5. Использование аналогового датчика влажности почвы. Подключение, программное чтения значений влажности почвы. Преимущества и недостатки других датчиков.
6. Использование аналогового датчика температуры. Подключение, программное чтения значений температуры. Преимущества и недостатки других датчиков.
7. Использование аналогового датчика освещённости. Подключение, программное чтения значений освещённости. Преимущества и недостатки других датчиков.
8. Сеть I2C, основы её функционирования.
9. Использование RTC (DS1302, DS1307, DS3231) и LCD1602.
10. Использование EEPROM.
11. Взаимодействие с интернет через
12. Разработка устройства мониторинга температуры в нескольких помещениях на базе датчиков температуры DS18B20 подключенных к одной линии с передачей данных по проводному Интернет на веб сервер.
13. Разработка устройства мониторинга температуры в нескольких помещениях на базе датчиков температуры DS18B20 подключенных к одной линии с передачей данных на веб сервер по сети WiFi.
14. Разработка устройства мониторинга температуры в нескольких помещениях на базе устройств WEMOS, датчиков температуры DS18B20 подключенных к одной линии с передачей данных по проводному Интернет на веб сервер.
15. Разработка устройства мониторинга температуры в нескольких помещениях на базе устройств WEMOS, датчиков температуры DS18B20 подключенных к одной линии с передачей данных по проводному Интернет через GSM модем.
16. Организация взаимодействие устройств IoT с Интернет и особенности разработки программного обеспечения для работы с Интернет посредством проводного Ethernet соединения.
17. Организация взаимодействие устройств IoT с Интернет и особенности разработки программного обеспечения для работы с Интернет посредством через устройства типа ESP-01.
18. Организация взаимодействие устройств IoT на базе микроконтроллеров семейства ESP-8266, с Интернет и особенности разработки программного обеспечения для их работы с Интернет.
19. Организация взаимодействие устройств IoT с Интернет и особенности разработки программного обеспечения для работы с Интернет посредством GSM модема.

6.2 Критерии оценивания компетенций:

Таблица 4

Карта критериев оценивания компетенций

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1	ОПК-7 - способность учитывать современные	Знает: архитектуру устройств ИВ и особенности сенсоров ИВ.	Практическая работа. Зачет.	Компетенция сформирована при правильности и

	тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	Умеет: разрабатывать устройства ИВ с учётом особенностей сенсоров ИВ и их взаимодействия с современными системами ИВ.		полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 "Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ"

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература:

1. Росляков, А. В. Интернет вещей : учебное пособие / А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков. — Самара : Поволжский государственный университет телекоммуникаций и информатики, 2015. — 135 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/71837.html (дата обращения: 01.12.2020). — Режим доступа: для авторизир. Пользователей

7.2 Дополнительная литература:

1. Дубков, И. С. Решение практических задач на базе технологии интернета вещей : учебное пособие / И. С. Дубков, П. С. Сташевский, И. Н. Яковина. — Новосибирск : Новосибирский государственный технический университет, 2017. — 80 с. — ISBN 978-5-7782-3161-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91510.html (дата обращения: 01.12.2020). — Режим доступа: для авторизир. пользователей

2. Боровский, А. С. Программирование микроконтроллера Arduino в информационно-управляющих системах : учебное пособие / А. С. Боровский, М. Ю. Шрейдер. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2017. — 113 с. — ISBN 978-5-7410-1853-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/78913.html (дата обращения: 01.12.2020). — Режим доступа: для авторизир. пользователей

7.3 Интернет-ресурсы:

1. Tinkercad [Электронный ресурс] - URL: https://www.tinkercad.com/dashboard (дата обращения: 25.05.2020).
2. Arduino[Электронный ресурс] - URL: https://www.arduino.cc (дата обращения: 25.05.2020).

3. Электронно-библиотечная система «Университетская библиотека он-лайн». - URL: http://biblioclub.ru
4. Электронно-библиотечная система издательства «Инфра». - URL: http://znanium.com.
5. eLIBRARY – Научная электронная библиотека (Москва). - URL: http://elibrary.ru

7.4 Современные профессиональные базы данных и информационные справочные системы:

- Межвузовская электронная библиотека (МЭБ). - URL: https://icdlib.nspu.ru/
- Национальная электронная библиотека. - URL: https://rusneb.ru/
- Institute of Electrical and Electronics Engineers, Inc (IEEE). - URL: https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Для проведение лекционных занятий используется техническое оборудование (проектор, микрофон, камера, контроллеры arduino, wemos D1R2, NodeMCU, Raspberry PI и другие, датчики и устройства (DS18B2, IButton, реле, расходные электронные компоненты (резисторы, диоды, светодиоды и т.д.) и другие, предусмотренные дисциплиной), сеть интернет, сайты https://tinkercad.com, https://youtube.com

- Лицензионное ПО:
  - Платформа для электронного обучения Microsoft Teams
  - Microsoft Imagine Academy (ранее Dreamspark): MS Visual Studio, MS SQL Server, ОС семейства MS Windows, MS Visio, MS Project
  - Microsoft Office
- Свободно распространяемое ПО:
  - Arduino IDE — https://www.arduino.cc/en/software
  - Autodesk Tinkercad - https://tinkercad.com/

При выполнении практических заданий, ведении лекций в качестве информационных технологий используется свободно распространяемое программное обеспечение Arduino IDE(https://arduino.cc), средства виртуального моделирования Tinkercad (https://tinkercad.com).

Доступ к компьютерным системам осуществляется на основе договоров ТюмГУ с создателями через компьютерную сеть университета (ЭБД, ЭБС, ЭБ), либо через виртуальные читальные залы университета, в частности, читальный зал для преподавателей и аспирантов ИБЦ (ЭБД РГБ).

Образовательные и научные он-лайн ресурсы (eLibrary, ЭБС IPRbooks, Znanium, BOOK.ru, Электронная библиотека диссертаций Российской государственной библиотеки и др.).

Платформа для электронного обучения Microsoft Teams.

Доступ к информационной образовательной среде осуществляется через локальную сеть ТюмГУ.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Для чтения лекций используется аудитория, оборудованная мультимедиа проектором и персональным компьютером. Для выполнения практических заданий и самостоятельной работы используется компьютерное оборудование (персональные компьютеры с подключением к Интернету), контроллеры arduino, wemos D1R2, NodeMCU, Raspberry PI и другие, датчики и устройства (DS18B20, IButton, реле, расходные электронные компоненты (резисторы, диоды, светодиоды и т.д.) и другие, предусмотренные дисциплиной), сеть интернет, сайты https://tinkercad.com, https://youtube.com

При выполнении практических заданий, ведении лекций в качестве информационных технологий используется свободно распространяемое программное обеспечение Arduino IDE(https://arduino.cc), средства виртуального моделирования Tinkercad (https://tinkercad.com).

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

ИСТОРИЯ СОЗДАНИЯ ТЕХНОЛОГИЙ ХРАНЕНИЯ, ПЕРЕДАЧИ И ЗАЩИТЫ ИНФОРМАЦИИ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Шабалин А.М История создания технологий хранения, передачи и защиты информации. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.
Рабочая программа дисциплины опубликована на сайте ТюмГУ: История создания технологий хранения, передачи и защиты информации [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Шабалин А.М, 2020.

1. Пояснительная записка

История создания технологий хранения, передачи и защиты информации обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.
Цель дисциплины «История создания технологий хранения, передачи и защиты информации» - является изложение истории развития мировой и отечественной мысли в области коммуникаций, а также истории защиты информации в средствах коммуникации.
Задачи курса - изучение:

- основных этапов истории развития коммуникаций терминологии;
- истории аналоговой коммуникации;
- истории и тенденции развития цифровых коммуникаций;
- основных технологий цифровых коммуникаций и их защищенность.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок 'Б1 Дисциплины (модули). Дисциплина по выбору. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: на знаниях мировой и отечественной истории, информатики, основ электротехники и алгебры, полученных в школе.

Дисциплина «История создания технологий хранения, передачи и защиты информации» способствует освоению следующих дисциплин: «Сети и системы передачи информации», «Системы управления базами данных», «Администрирование операционных систем»

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-5 - способность понимать социальную значимость своей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики		знает - свойства информации, подлежащие закрытию; умеет - ориентироваться в истории технологий передачи информации,
ОПК-3 - способность понимать значение информации в развитии современного общества, применять достижения информационных		знает - этапы развития средств и технологий коммуникаций; умеет - методах защиты информации в контексте исторического развития.

технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации		
ПК-10 - способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		знает -историю развития информационного противоборства в России и мире. умеет - оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
ПК-12 - способность проводить инструментальный мониторинг защищенности компьютерных систем		знает - основные технологии передачи цифровой информации; умеет - проводить инструментальный мониторинг защищенности компьютерных систем
ПК-17 - способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение		знает - назначение основных устройств (маршрутизаторов, коммутаторов) обеспечивающих передачу цифровой информации. умеет - производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение
ПК-18 - способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности		знает - основные стандарты, используемые при передаче цифровой информации; умеет - производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности

компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
ПК-19 - способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации		знает - основные технологии защиты информации. умеет - производить проверки технического состояния и профилактические осмотры технических средств защиты информации
ПК-20 - способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций		знает - основы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций умеет - выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций
ПК-3 - способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности		знает основы безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности умеет -проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности
ПК-9 - способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы		знает -основы при аттестации объектов с учетом требований к уровню защищенности компьютерной системы умеет - участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы

ПСК-3.1 - способность использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем		знает - основы использования современных критерии и стандарты для анализа безопасности распределенных компьютерных систем умеет - создавать, безопасное подключение LAN к Интернет.
ПСК-3.2 - способность анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем		Знает основы анализа защиты информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем умеет - создавать и настраивать LAN сети.

* не предусмотрено

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		1 семестр
Общий объем зач. ед.	3	3
час.	108	108
Из них:		
Часы аудиторной работы (всего):	72	72
Лекции	36	36
Практические занятия	36	36
Лабораторные/практические занятия по подгруппам		
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	36	36
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет

3. Система оценивания

3.1.

Форма проведения зачета – контрольная работа. Продолжительность выполнения контрольной работы - астрономический час. Контрольная работа включает два задания. Каждое задание оценивается максимально в 50 баллов. Фактическое количество баллов определяется отношением правильно сформированных показателей к общему количеству показателей, заполняемым по конкретным исходным данным. Правильно сформированный

показатель – показатель, отраженный по той статье и в том количественном выражении, которые определены нормативными документами

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			
			Лекции	Практические занятия	Лабораторные практические занятия по подгруппам	Иные виды контактной работы
1	2	3	4	5	6	7
1.	Введение в технологии Защищенных коммуникаций	12	2	2	0	0
2.	3 этапа развития защищенных коммуникаций.	12	4	4	0	0
3.	Локальные, корпоративные и глобальные сети.	12	4	4	0	0
4.	Сетевая адресация. IP адреса и маска подсети.	12	4	4	0	0
5.	Сетевые службы	12	4	4	0	0
6.	Беспроводные технологии.	12	6	6	0	0
7.	Основы безопасности цифровых коммуникаций.	12	4	4	0	0
8.	Структура, адресация и настройка сети. Маршрутизация.	12	4	4	0	0
9.	Коммутируемая архитектура Корпоративные сети.	12	4	4	0	0
	Итого (часов)	108	36	36		0

4.2. Содержание дисциплины (*модуля*) по темам

1. Введение в технологии защищенных коммуникаций. Основные понятия и определения. Типы коммуникаций. Виды информации, подлежащие закрытию, их модели и свойства. Основные этапы становления защищенных коммуникаций. Специальная терминология.

2. 3 этапа развития защищенных коммуникаций. Наивный подход. Криптография. Кодирование и скрытие информации. Понятие о стеганографии. Аналоговые технологии передачи информации. Цифровая информация. Аппаратное обеспечение – виды сетевых адаптеров. Программное обеспечение. Операционные системы

3. Локальные, корпоративные и глобальные сети. Возникновение LAN. Топологии, архитектуры и технологии. Ethernet. Стандарты. История разработки оборудования для сетевого взаимодействия

4. Сетевая адресация. IP адреса и маска подсети. Классы IP адресов и маски подсетей по умолчанию. Статический адрес. Динамические адреса. Протокол Dynamic Host Configuration Protocol (DHCP).

5. Сетевые службы DNS, DHCP, FTP, Telnet, Web, Электронная почта.

6. Беспроводные технологии. Электромагнитные волны. Инфракрасное (ИК) излучение. Радиочастотный диапазон (РЧ). Преимущество и ограничения беспроводных технологий. Стандарты IEEE 802.11. Идентификатор беспроводной сети SSID.

7. Основы безопасности цифровых коммуникаций. Внешние угрозы. Внутренние угрозы. Социотехника. Фишинг. Телефонный фишинг Вирусы, черви, троянские кони. DoS-атаки. Политика безопасности Антивирусное ПО Межсетевой экран. Демилитаризованная зона (DMZ). Развитие гражданской криптографии в СССР и России. ИКСИ Академии ФСБ России.

8. Структура, адресация и настройка сети маршрутизация. Начальная конфигурация. Режимы команд CLI. Статическая маршрутизация. NAT и PAT.

9. Корпоративные сети. Коммутация. Режимы потоков трафика. Виртуальные сети Описание сети. Проектирование поддержки удаленного сотрудника.

Планы практических занятий

Практическая работа 1 Packet Tracer. Навигация по IOS

Отработка навыков, необходимых для навигации по операционной системе Cisco IOS, включая различные пользовательские режимы доступа, всевозможные режимы конфигурации.

Практическая работа 2 Packet Tracer - Configure Initial Switch Settings

Настройка базовые параметры коммутатора.

Практическая работа 3 Packet Tracer. Создание основных подключений

Создание базовой конфигурации коммутатора, основных подключений, настройка IP-адресации на коммутаторах и ПК.

Практическая работа 4 Packet Tracer - Basic Switch and End Device Configuration

Настройка исходных параметров на двух коммутаторах под управлением Cisco IOS, параметров IP-адресации на узлах для создания сквозного подключения

Практическая работа 5 Packet Tracer - Изучение моделей TCP/IP и OSI в действии

Изучение HTTP-трафика. Отображение элементов семейства протоколов TCP/IP

Практическая работа 6 Packet Tracer - Подключение проводной и беспроводной локальных сетей

Подключение к облаку. Подключение маршрутизатора Router0. Проверка подключений

Практическая работа 7 Packet Tracer - Подключение физического уровня

Определение физических характеристик межсетевых устройств. Выбор подходящих модулей для подключения

Практическая работа 8 Cisco Packet Tracer. Определение MAC- и IP-адресов

Сбор информации PDU для локальной сети связи. Сбор информации PDU для удаленной сетевой связи

Практическая работа 9 Cisco Packet Tracer. Изучение таблицы ARP

Анализ ARP-запроса. Изучение таблицы MAC-адресов коммутатора. Анализ процесса ARP в удаленных подключениях

Практическая работа 10 Packet Tracer - Обнаружение соседних IPv6 устройств

Локальная сеть обнаружения соседей IPv6. Удаленная сеть обнаружения соседей IPv6

Практическая работа 11 Cisco Packet Tracer. Настройка исходных параметров маршрутизатора

Проверка конфигурации маршрутизатора по умолчанию. Настройка и проверка начальной конфигурации маршрутизатора.

Практическая работа 12 Cisco Packet Tracer. Подключение маршрутизатора к локальной сети (LAN)

Отображение сведений о маршрутизаторе. Настройка интерфейсов маршрутизатора. Проверка конфигурации

Практическая работа 13 Cisco Packet Tracer. Устранение неполадок, связанных со шлюзом по умолчанию

Проверка сетевой документации и устранение проблем. Внедрение, проверка и документирование решений

Лабораторная работа 14 Packet Tracer - базовая конфигурация устройства

Составление сетевой документации. Настройка базовых параметров маршрутизатора и коммутатора. Проверка подключения и устранение неполадок.

Практическая работа 15 Packet Tracer — Разделение IPv4-сети на подсети

Разработка схемы разделения сети на подсети. Настройка устройств. Проверка сети и устранение неполадок.

Практическая работа 16 Packet Tracer. Сценарий разделения на подсети

Разработка схемы IP-адресации. Назначение сетевым устройствам IP-адресов и проверка подключения.

Практическая работа 17 Packet Tracer - Практика проектирования и внедрения VLSM

Изучение требований к сети. Разработка схемы адресации VLSM. Назначение сетевым устройствам IP-адресов и проверка подключения.

Практическая работа 18 Packet Tracer - Разработка и реализация схемы адресации VLSM

Разработка схемы IP-адресации VLSM с учетом требований. Настройка адресации на сетевых устройствах и хостах. Проверка IP-подключения. Поиск и устранение неполадок подключения

Образцы средств для проведения текущего контроля

Проверка качества подготовки в течение семестра предполагает следующие виды промежуточного контроля:

А) модели сети на Packet Tracer;

Б) выполнение расчетной работы на компьютере в группах;

В) подготовка студентом перевода специального текста с иностранного языка на русский.

Примерные темы расчетных работ - моделей сети для Packet Tracer:

1) связь двух компьютеров напрямую.

2) LAN и более 3 х компьютеров.

3) Беспроводная LAN.
4). Настройка маршрутизатора
5). Подключение двух LAN
6). Подключение к ISP
7). Моделирование подключения к Интернет
8) Администрирование и поиск ошибок.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Введение в технологии защищенных коммуникаций	Чтение обязательной литературы, подготовка к практическим занятиям
2.	3 этапа развития защищенных коммуникаций.	Чтение обязательной литературы, подготовка к практическим занятиям
3.	Локальные, корпоративные и глобальные сети.	Чтение обязательной литературы, подготовка к практическим занятиям
4.	Сетевая адресация. IP адреса и маска подсети.	Чтение обязательной литературы, подготовка к практическим занятиям
5.	Сетевые службы	Чтение обязательной литературы, подготовка к практическим занятиям
6.	Беспроводные технологии.	Чтение обязательной литературы, подготовка к практическим занятиям
7.	Основы безопасности цифровых коммуникаций.	Чтение обязательной литературы, подготовка к практическим занятиям
8.	Структура, адресация и настройка сети. Маршрутизация.	Чтение обязательной литературы, подготовка к практическим занятиям
9.	Коммутируемая архитектура Корпоративные сети.	Чтение обязательной литературы, подготовка к практическим занятиям

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение рекомендованной основной и дополнительной литературы.
3. Разбор примеров практических работ.

Контроль за самостоятельной работой осуществляется при выполнении обучающимся теста, контрольной работы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения зачета – контрольная работа.

Пример заданий на контрольную работу.

1)Маршрутизатор с двумя интерфейсами LAN, двумя интерфейсами WAN и одним настроенным интерфейсом обратной связи (loopback) работает с протоколом маршрутизации OSPF. Что процесс OSPF маршрутизатора использует для назначения маршрутизатору идентификатора?

- IP-адрес интерфейса, настроенного с приоритетом 0
- идентификатор области OSPF, заданный на интерфейсе с самым высоким IP-адресом
- IP-адрес интерфейса обратной связи
- самый высокий IP-адрес, настроенный на интерфейсах LAN
- самый высокий IP-адрес на интерфейсах WAN

2) Какие меры используются для предотвращения петель маршрутизации в сетях, в которых используются протоколы маршрутизации на базе вектора расстояния? (Выберите два варианта.)

- объявления о состоянии канала (LSA)
- протокол связующего дерева
- дерево SPF
- разделение горизонта (split horizon)
- таймеры удержания (hold-down timer)

3) В каком варианте представлено наилучшее описание протоколов маршрутизации на базе вектора расстояния?

- В качестве единственной метрики они используют подсчет переходов (hop).
- Они отправляют обновления только при добавлении новой сети.
- Они отправляют свои таблицы маршрутизации к напрямую подключенным соседним маршрутизаторам.
- Они рассылают обновление маршрутизации по всей сети.

6.2. **Критерии оценивания компетенций:**

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОК-5 - способность понимать социальную значимость своей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства,	знает - свойства информации, подлежащие закрытию; умеет - ориентироваться в истории технологий передачи информации	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

	соблюдать нормы профессиональной этики			
2.	ОПК-3 - способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации	знает - этапы развития средств и технологий коммуникаций; умеет - методах защиты информации в контексте исторического развития.	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
3.	ПК-10 - способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	знает -историю развития информационного противоборства в России и мире. умеет - оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

4.	ПК-12 - способность проводить инструментальный мониторинг защищенности компьютерных систем	знает - основные технологии передачи цифровой информации; умеет - проводить инструментальный мониторинг защищенности компьютерных систем	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
5.	ПК-17 - способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение	знает - назначение основных устройств (маршрутизаторов, коммутаторов) обеспечивающих передачу цифровой информации. умеет - производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
6.	ПК-18 - способность производить установку, наладку, тестирование и обслуживание современных программно-	знает - основные стандарты, используемые при передаче цифровой информации; умеет - производить установку, наладку,	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий,	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий.

	аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографическо й защиты информации	тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	- Задачи	Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
7.	ПК-19 - способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации	знает - основные технологии защиты информации. умеет - производить проверки технического состояния и профилактические осмотры технических средств защиты информации	- Опрос на практическо м занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
8.	ПК-20 - способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	знает - основы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций умеет - выполнять работы по восстановлению работоспособности	- Опрос на практическо м занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем

		средств защиты информации при возникновении нештатных ситуаций		контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
9.	ПК-3 - способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	знает основы безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности умеет -проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
10.	ПК-9 - способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	знает -основы при аттестации объектов с учетом требований к уровню защищенности компьютерной системы умеет - участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
11.	ПСК-3.1 - способность использовать современные критерии и стандарты для	знает - основы использования современных критерии и стандарты для	- Опрос на практическом занятии - Тест закрытый, 10 заданий,	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания

	анализа безопасности распределенных компьютерных систем	анализа безопасности распределенных компьютерных систем умеет - создавать, безопасное подключение LAN к Интернет.	- Тест открытый, 10 заданий, - Задачи	вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
12.	ПСК-3.2 - способность анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем	Знает основы анализа защиты информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем умеет - создавать и настраивать LAN сети.	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 368 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100522 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

7.2. Дополнительная литература:

1. Кияев, В. И. Безопасность информационных систем : учебное пособие / В. И. Кияев, О. Н. Граничин. — 2-е изд. — Москва : ИНТУИТ, 2016. — 191 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100580 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

2. Олифер, В. Г. Основы сетей передачи данных : учебное пособие / В. Г. Олифер, Н. А. Олифер. — 2-е изд. — Москва : ИНТУИТ, 2016. — 219 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100346 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

3. Построение коммутируемых компьютерных сетей : учебное пособие / Е. В. Смирнова, И. В. Баскаков, А. В. Пролетарский, Р. А. Федотов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 428 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100370 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

7.3. Интернет-ресурсы
Интернет ресурсы Academy Cisco http://netacad.com

7.4 Современные профессиональные базы данных и информационные справочные системы:
Базы данных
- Institute of Electrical and Electronics Engineers, Inc (IEEE) https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) https://icdlib.nspu.ru/
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА https://rusneb.ru/
- Справочная правовая система КонсультантПлюс http://www.consultant.ru/

Наименование ПО
- Microsoft Office 365
- "Microsoft Imagine Academy (ранее Dreamspark):MS Visual Studio, MS SQL Server,ОС семейства MS Windows,MS Visio, MS Project"

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)
эмулятор сетей PacketTracer.версия 7.x;
эмулятор сетей GNS3 2.*
эмулятор сетей eNSP 1.3.*
гипервизор Oracle Virtual Box 5.*
платформа для электронного обучения Microsoft Teams
Интернет, доступ в информационно-образовательную среду ТюмГУ, включающую в себя доступ к учебным планам и рабочим программам, к изданиям электронной библиотечной системы.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)
Компьютерный класс с выходом в интернет и стандартное лабораторное и периферийное оборудование классом не ниже чем в приведенной ниже конфигурации.
• 3 маршрутизатора Cisco 2801 с Base IP IOS, 128 Мбайт DRAM, 32 Мбайта флэш-памяти и модулями HWIC-2A/S;
• 3 коммутатора Cisco Catalyst 2960;
• Набор последовательных кабелей и витой пары;
• 2 беспроводных маршрутизатора Linksys (предпочтительно Linksys WRT150N; допустимо использование моделей WRT54G, WRT300N и WRT350N) или аналогичные устройства SOHO;
Для проведения лекционных и практических занятий необходим проектор с разрешением не менее 800x1200 подключенный к компьютеру с выходом в Интернет.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Атманских М.Б., Ниссенбаум О.В. Криптографические методы защиты информации. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Криптографические методы защиты информации [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Атманских М.Б, Ниссенбаум О.В. 2020.

1. Пояснительная записка

Студент приобретет теоретические знания об организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; практическое освоение приемов и методов программной реализации криптографических алгоритмов; владение основами алгоритмизации и автоматизации выполнения работ. В ходе выполнения практических работ на занятиях с разделением на подгруппы научится применять математические методы, используемые в криптографии в соответствии с российскими и международными стандартами, освоит основные принципы разработки шифров.

Программа дисциплины ориентирована на достижение следующих целей: · приобретение основных знаний о методах криптографических преобразований информации и методах криптоанализа современных шифров; овладение умением чтения российских и зарубежных криптографических стандартов; · воспитание ответственности к профессиональной деятельности, воспитание самообразования; · развитие навыков программной реализации криптографических алгоритмов; · формирование готовности использовать приобретенные знания в профессиональной деятельности.

Исходя из целей, в программе дисциплины «Криптографические методы защиты информации» предусматриваются задачи: · сформировать у обучающегося необходимый объем знаний о принципах разработки шифров и методах их криптоанализа; · научить читать базовые российские и зарубежные криптографические стандарты; · развить навыки программной реализации криптографических алгоритмов; · сформировать умения применять знания о математических методах построения криптографических средств защиты информации на практике.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Алгебра и геометрия», «Языки программирования», «Информатика», «Введение в теорию вероятностей и математическую статистику», «Теоретико-числовые методы в криптографии».

Дисциплина «Криптографические методы защиты информации» способствует освоению следующих дисциплин: «Криптографические протоколы», «Безопасность интернета вещей», «Безопасность баз данных», «Разработка и защита медицинских информационных систем».

1.2. **Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)**

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-8 - способность к самоорганизации и самообразованию		знать: - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; уметь: - самостоятельно строить процесс овладения информацией,

		отобранной и структурированной для выполнения профессиональной деятельности.
ПК-5 - способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		знать: - внутреннюю структуру криптографических алгоритмов, их область применения и свойства; внутреннее содержание отечественных криптографических стандартов, их характеристики по сравнению с зарубежными. уметь: - самостоятельно реализовать стандартный криптографический алгоритм; применять на практике отечественные стандарт.
ПК-10 - способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		знать: - основы теорий секретности и имитостойкости, тесты на простоту, общие приемы дифференциального и линейного криптоанализа, основные алгоритмы факторизации и дискретного логарифмирования. Математические модели и свойства криптосистем. уметь: - показать полноту и корректность криптосистемы, получать криптографические ключи, построить математическую модель и вычислить вероятностные характеристики криптосистемы.

* не предусмотрено

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		5 семестр
Общий объем зач. ед.	4	4
час.	144	144
Из них:		
Часы аудиторной работы (всего):	90	90
Лекции	54	54
Практические занятия		
Лабораторные/практические занятия по подгруппам	36	36

Часы внеаудиторной работы, включая самостоятельную работу обучающегося	54	54
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		экзамен

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной) и традиционной (4-балльной) систем оценок.

Экзаменационная оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических работ на занятиях с разделением на подгруппы. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать экзамен.

Экзаменационная оценка студента в рамках традиционной системы оценок выставляется на основе ответа студента на теоретические вопросы. Эта оценка характеризует уровень знаний, умений и навыков, приобретенных студентом в ходе изучения дисциплины.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса и практическое задание из пройденных тем на усмотрение преподавателя. Для получения оценки «удовлетворительно» студентом должно быть сдано минимум 4 практические работы на занятиях с разделением на подгруппы и сделан ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен сдать минимум 8 практических работ на занятиях с разделением на подгруппы и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности, может воспроизвести общую схему описываемого криптографического алгоритма, знает и понимает основные свойства, слабости и область применения. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты, допускается отсутствие доказательств теорем, подробного описания транзакций протоколов, если приведена их суть. Для получения оценки «отлично» студент должен сдать минимум 12 практических работ на занятиях с разделением на подгруппы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. В ответе должны быть приведены доказательства всех теорем и(или) подробное описание шагов алгоритма.

Примечание. Студент, желающий исправить экзаменационную оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Введение в криптографию.	6	2	0	1	0
2.	История криптографии. Исторические шифры.	8	4	0	2	0
3.	Математическая модель шифра. Теория секретности Шеннона	12	6	0	4	0
4.	Блочные шифры	22	8	0	6	0
5.	Псевдослучайные последовательности и поточные шифры.	18	6	0	4	0
6.	Теория имитостойкости Симмонса и криптографические хэш-функции.	20	8	0	6	0
7.	Асимметричные (с открытым ключом) шифры	16	6	0	4	0
8.	Схемы цифровой подписи.	16	6	0	4	0
9.	Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе	20	6	0	4	0
10.	Введение в криптографические протоколы	6	2	0	1	0
	Итого (часов)	144	54	0	36	2

4.2. Содержание дисциплины (*модуля*) по темам

Модуль 1. Основы криптографии.

1. Введение в криптографию. Основные понятия и определения. Виды криптосистем. Задачи, решаемые методами криптографии. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.

2. История криптографии. Исторические шифры. Основные этапы становления криптографии как науки. Классификация шифров. Шифры замены, перестановки, гаммирования. Композиции шифров. Примеры исторических ручных и машинных шифров. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Шифр «Решетка». Шифр Вернама. Enigma. Шифр Хейглина. Способы их вскрытия. Блочные и поточные шифры.

3. Математическая модель шифра. Теория секретности Шеннона. Алгебраическая модель, вероятностная модель. Атаки и угрозы шифрам. Вычислительная и теоретическая

стойкость. Теоретико-информационный подход к оценке стойкости шифров. Криптографическая стойкость шифров. Совершенные шифры. Энтропийные характеристики шифров. Идеальные шифры. Избыточность языка. Оценка числа ложных ключей и расстояние единственности. Безусловно стойкие и вычислительно стойкие шифры. Вопросы практической стойкости.

Модуль 2. Симметричные криптосистемы.

4. Блочные шифры. Понятие о блочном шифре. Замены и перестановки. S-P сеть. Лавинный эффект. Сеть Файстеля. Шифр ГОСТ 28147-89. Шифры SQUARE, AES. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ. Режимы шифрования. Многократное шифрование и атака «встреча посередине». Композиция блочных шифров.

5. Псевдослучайные последовательности и поточные шифры. Характеристики генераторов псевдослучайных последовательностей (ПСП, ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры. Регистры сдвига с обратной линейной связью (РСЛОС). ПСГ на основе РСЛОС. Шифр Trivium. Нелинейные регистры сдвига. Другие поточные шифры – RC4.

6. Теория имитостойкости Симмонса и криптографические хэш-функции. Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Связь между имитостойкостью по Симмонсу и секретностью по Шеннону. Понятие кода аутентификации и его свойства имитостойкости и секретности. Назначение и конструкция кодов аутентификации и защитных контрольных сумм. Требования к хэш-функциям. Криптографическая стойкость хэш-функций. Коллизии. Применение хэш-функций. Подходы к проектированию хэш-функций. Алгоритмы выработки хэш-функций. Хэш-функции на основе блочного шифра. Стандарты на хэш-функции: ГОСТ Р 34.11-94, SHA-1. Схема Меркла-Дамгарда и ГОСТ Р 34.11-2012. Концепция «губка» и SHA-3. Коды аутентификации и способы их построения. HMAC.

Модуль 3. Асимметричные криптосистемы и протоколы.

7. Асимметричные (с открытым ключом) шифры. Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях. Криптосистема Диффи-Хэллмана. Криптосистемы RSA, Эль-Гамаля, Рабина, Гольдвассер-Микали, Блюма-Гольдвассер. Рюкзачные шифры. Криптосистемы с открытым ключом, основанные на линейных кодах. Преимущества и недостатки асимметричных систем шифрования. Генерация ключевой информации для асимметричных криптосистем. Вероятностные тесты на простоту. Доказуемо простые числа. Нахождение порождающего элемента и элемента заданного порядка.

8. Схемы цифровой подписи. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП. Алгоритмы ЭЦП: RSA, Эль-Гамаля, ФиатаШамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ванАнтверпена. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.

9. Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе. Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка. Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра (ЭЦП) в Zp к шифру (ЭЦП) на эллиптической кривой. Шифр Эль-Гамаля на эллиптической кривой. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ECDSA.

10. Введение в криптографические протоколы. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Парольные схемы и протоколы "рукопожатия". Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей. Протоколы предварительного распределения ключей.

Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации. Вопросы организации сетей засекреченной связи. Доказательства с нулевым разглашением. Разделение секрета. Протоколы подбрасывания монеты. Построение протоколов с нулевым разглашением на основе NP-сложных задач.

Темы практических работ на занятиях с разделением на подгруппы

Модуль 1. Основы криптографии.

Тема 1: Введение в криптографию.

1.Свойства информации. Ситуационные задачи на определение свойств информации, подлежащей криптографическому преобразованию.

Тема 2: История криптографии. Исторические шифры.

2. Исторические шифры и их криптоанализ. Компьютерная реализация и вскрытие шифров замены.

Тема 3: Математическая модель шифра. Теория секретности Шеннона

3.Вероятностные характеристики текстов. Определение избыточности текста, языка. Расчет параметров шифров. Расстояние единственности, определение количества ложных ключей.

Модуль 2. Симметричные криптосистемы.

Тема 4: Блочные шифры.

4. Блочные шифры. Программная реализация 4-битовых замен в 32-битовом слове согласно таблицам замены.

5. Блочные шифры. Программная реализация ГОСТ 28147-89.

6. Многочлены над Z_2 и блочный шифр AES. Программная реализация операций над байтами в AES.

Тема 5: Псевдослучайные последовательности и поточные шифры.

7. Псевдослучайные генераторы на основе РСЛОС. Оценка свойств гаммы шифра. Программная реализация РСЛОС.

8. Программная реализация генератора на основе РСЛОС по вариантам.

Тема 6: Теория имитостойкости Симмонса и криптографические хэш-функции.

9. Вычисление параметров имитостойкости, помехоустойчивости шифров.

10. Построение криптографической хэш-функции на основе блочного шифра и исследование ее свойств методами математической статистики и теории информации.

Модуль 3. Асимметричные криптосистемы и протоколы.

Тема 7: Асимметричные (с открытым ключом) шифры.

11. Генерация больших простых чисел для асимметричных криптосистем с помощью вероятностных тестов (программная реализация по вариантам).

12. Построение доказуемо простых больших простых чисел для асимметричных криптосистем (программная реализация по вариантам).

13. Вычисления в Zn. Программная реализация шифр с открытым ключом (по вариантам): RSA, Эль-Гамаля, Шамира, Диффи-Хэллмана, Рабина, Гольдвассер-Микали, Блюма-Гольдвассер, Меркла-Хэллмана.

Тема 8: Схемы цифровой подписи.

14. Программная реализация процедуры генерации доказуемо простых чисел (по вариантам).

15. Программная реализация схемы ЭЦП (по вариантам): RSA, Эль-Гамаля и ее варианты, Фиата-Шамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ван-Антверпена.

Тема 9: Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе.

16. Эллиптические кривые над конечным полем. Программная реализация операций над точками эллиптической кривой над Zp.

17. Преобразование криптосистемы над Zp в криптосистему на эллиптической кривой.

18. Программная реализация криптосистемы на эллиптической кривой.

Тема 10: Введение в криптографические протоколы.

19. Изучение примитивных протоколов.

Образцы средств для проведения текущего контроля

Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках рейтинговой (100-бальной) системы оценок.

1. Примеры материалов к практическим занятиям с разделением на подгруппы

Тема 7: Асимметричные (с открытым ключом) шифры.

11. Генерация больших простых чисел для асимметричных криптосистем с помощью вероятностных тестов (программная реализация по вариантам).

Все методы генерации простых чисел разделяются на две группы: методы, генерирующие число, являющееся простым с высокой степенью вероятности (т.н. probability methods) и методы, генерирующие числа, являющиеся доказуемо простыми (т.н. provability methods).

«Вероятно простые» числа генерируются методом случайного поиска среди всех целых (нечетных) чисел заданного диапазона и проверкой их на простоту вероятностными методами. Доказуемо простые числа могут быть найдены либо случайным поиском и последующей проверкой детерминированным тестом, либо построением специальными методами.

Эффективность случайного поиска зависит от вероятности того, что наугад взятое число из данного диапазона является простым. Если в заданном диапазоне отсутствуют простые числа, или их крайне мало, то и случайный поиск лишен смысла.

Случайный поиск числа в заданном диапазоне.

Для того чтобы оценить время, которое придется затратить на случайный поиск в заданном диапазоне, необходимо знать, сколько примерно простых чисел в этом диапазоне содержится. Конечно, точное распределение простых чисел в N неизвестно, но некоторые сведения об этом распределении у современной математики имеются. Более точно на вопрос о распределении простых чисел в N отвечает асимптотический закон распределения простых чисел.

Итак, обозначим $\pi(x)$ – количество простых чисел, меньших или равных x. Тогда справедлив

Асимптотический закон распределения простых чисел: $\frac{ln ln\, x}{x} = 1$

Другими словами, при $x \to \infty$, $\pi(x) \to x/\ln x$.

Зная количество простых чисел в диапазоне, можно вычислить вероятность выбора простого числа, среднее ожидаемое количество чисел, которые потребуется перебрать и т.п.

Пример

Оценим вероятность, с которой наугад выбранное нечетное 32-х битовое число (старший бит = 1) является простым.

Наибольшее такое число – это (2^{32}-1), а наименьшее – (2^{31}+1). Таким образом, согласно асимптотическому закону, всего простых чисел в заданном диапазоне примерно $\pi(2^{32})$–$\pi(2^{31}) \approx \frac{2^{32}}{ln\,ln\,2^{32}} - \frac{2^{31}}{ln\,ln\,2^{31}} = \frac{2^{32}}{2} - \frac{2^{31}}{2} = \frac{2^{31}}{ln\,ln\,2}\frac{2}{32}\frac{1}{31} = \frac{2^{31}}{ln\,ln\,2}\frac{15}{2^4 31} = \frac{15}{31}\frac{2^{27}}{ln\,ln\,2}$

Всего чисел в диапазоне поиска 230. Таким образом, искомая вероятность есть $p = \frac{(2^{32})(2^{31})}{2^{30}} \approx \frac{15\ 2^{27}}{31\ 2^{30}\ ln\,ln\,2} = \frac{15}{31\ 2^3\ ln\,ln\,2} \approx \frac{1}{11.46}$

Итак, полученная вероятность достаточно велика. Выясним, сколько чисел из данного диапазона требуется перебрать, чтобы получить хотя бы одно простое с вероятностью не менее 0,9.

Эта величина n будет найдена из выражения

$$1 - (1 - p)^n \geq 0{,}9$$

Или $$n \geq 0{,}1$$

При p= $\frac{1}{11.46}$ получим n≥25.21.

Итак, n=26.

Среднее ожидаемое количество чисел, которое потребуется перебрать, чтобы получить простое число, составляет

$$k = \frac{1}{p}$$

В нашем случае, k=11.46.

Вероятностные тесты на простоту

Тесты на простоту, которые позволяют эффективно определять, является ли данное число простым, но с помощью которых нельзя строго доказать составность числа, получили название вероятностных тестов.

Одним их таких тестов является тест Ферма, основанный на теореме Эйлера.

2.2.1. Тест Ферма на простоту

Вход: число n – для проверки на простоту, t – параметр надежности.

1. Повторяем t раз:
   а) Случайно выбираем a ∈ {2,…, n-2};
   б) Если a n–1 mod n ≠ 1 ⇒ «n – составное». Выход.
2. «n – простое с вероятностью $1- \varepsilon^t$ »

Этот тест может принять составное число за простое, но не наоборот.

Вероятность ошибки есть ε^t, где $\varepsilon \leq \frac{(n)}{n}$,где ϕ(n) - функция Эйлера.

В случае составного числа n, имеющего только большие делители, ε ≈ 1 , то есть существуют числа, для которых вероятность ошибки при проверке их на простоту тестом Ферма близка к 1.

Рекомендуется выбирать t около 50.

Замечание. Для теста Ферма существуют так называемые числа Кармайкла – такие составные числа, что ∀ a: (a,n) = 1 ⇒ $a^{n-1} \equiv 1 (\text{mod } n)$. То есть числа Кармайкла – это такие составные числа, которые всегда принимаются тестом Ферма за простые, несмотря на то, как велико число t – параметр надежности теста.

Пример использования теста:

N=43, t=2

1-я итерация

а) a=35

б) 35^{42} mod 43 =1

2-я итерация

а) a=13

б) 1342 mod 43 =1

Выход: n-простое число

Тест Соловея-Штрассена

Этот тест основан на различии между символами Якоби (знаменатель которого – составное число) и Лежандра (знаменатель – простое число). Дело в том, что алгоритм вычисления этих двух символов одинаков, но для символа Лежандра выполняется критерий Эйлера, а для символа Якоби – нет.

Критерий Эйлера: $\frac{a}{n} = a^{\frac{n-1}{2}} (mod\ n)$

Тест Соловея-Штрассена:

Вход: n – нечетное, t – параметр надежности.

1. Повторить t раз:

1.1 Случайно выбираем a ∈ {2,…, n-2};

1.2. Если (a,n) ≠ 1 ⇒ “n – составное”. Выход.

1.3. Вычисляем $r = \frac{a}{n}$, $s = a^{\frac{n-1}{2}} (mod\ n)$

1.4. Если r ≠s ⇒“n –составное ”. Выход.

2. “n –простое с вероятностью $1- \varepsilon^t$”. Выход.

Как и тест Ферма, этот тест может принять составное число за простое, но не наоборот. Вероятность ошибки (то есть вероятность принять составное число за простое) составляет ε^t , где t – число итераций теста, параметр надежности,

$$\varepsilon \leq \frac{(n)}{2n} < \frac{1}{2}$$

Как видим, оценка надежности теста Соловея–Штрассена гораздо лучше, чем для теста Ферма, даже в том случае, когда φ(n) ненамного меньше n.

В тесте вычисляется символ Якоби $r = \frac{a}{n}$, для чего используется следующий алгоритм.

Алгоритм вычисления символа Якоби:

Вход: n - числитель, m – знаменатель символа Якоби. m – нечетное число, n, m>0.

Задаем r=1.

1. Если (n,m)≠1, то r :=0. Идти на Выход.
2. n:=n mod m.
3. Представить n как $n=2^k n_1$, где n_1 – нечетное число. k:=k mod 2, n:= n_1.
4. Если k=1, то если m mod 8 = 3 или m mod 8 = 5, то r := –r .
5. Если n=1, то идти на Выход.

6. Если n=m—1, и m mod 4 = 1, то идти на Выход.

Если n=m—1, и m mod 4 = 3, то r := –r, и идти на Выход.

7. n↔m; r :=$r \cdot (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$ Идти на Шаг 2.

Выход. r – символ Якоби.

Пример вычисления символа Якоби:

$$\frac{219}{383} = -\frac{383}{219} = -\frac{164}{219} = -\left(\frac{4}{219}\right)\left(\frac{41}{219}\right) = -\frac{219}{41} = -\frac{14}{41} = -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -\frac{7}{41} == -\frac{41}{7}$$
$$= -\frac{6}{7} = -\frac{-1}{7} = 1$$

Пример применения теста Соловея-Штрассена:

N=43, t=2

1-я итерация :

1.1 a=30

1.2 НОД(30,43)=1

1.3 r= $\frac{30}{43}$= -1, s= $30^{\frac{43-1}{2}}$ mod 43 = -1

1.4 r=s

2-я итерация :

1.1 a=4

1.2 НОД(4,43)=1

1.3 r= $\frac{4}{43}$ =1, s= $4^{\frac{43-1}{2}}$ mod 43 = 1

1.4 r=s

2. “43 –простое с вероятностью 1— ε^2 ”. Выход.

Тест на простоту Миллера-Рабина.

Тест Миллера-Рабина, как и тесты Ферма и Соловея-Штрассена, строит вероятно простые числа, то есть число, опознанное этим тестом как простое, может с некоторой малой вероятностью оказаться составным, однако вероятность ошибки у теста МиллераРабина гораздо ниже, чем у первых двух тестов. Как правило, для опознания простого числа достаточно одной итерации теста, но все же рекомендуемое количество итераций – пять.

Тест Миллера-Рабина основан на двух важных фактах:

1) Согласно теореме Ферма, если n – простое число, то для любого a: 0<a выполняется $a^{n-1} \equiv 1(mod\ n)$;

2) Если n – простое число, то сравнение $x^2 \equiv 1(mod\ n)$ имеет только тривиальные корни x≡±1(mod n), а если n – составное, то такое сравнение имеет несколько корней помимо тривиальных.

Тест Миллера-Рабина:

Вход: n=2^sr+1 – нечетное число, проверяемое на простоту, s≥0, r – нечетное. t - количество итераций, параметр надежности.

1. Повторить t раз следующие шаги:

1.1. Случайным образом выбрать a ∈ {2,…, n-2};

1.2. Построить последовательность b_0, b_1,…, b_s, по правилу: b_0=a^r mod n, b_j=$(b_{j-1})^2$mod n, j=1,2,…,s.

1.3. Если в построенной последовательности не встретилась «1», то идти на Выход с сообщением «n - составное».

1.4. Если перед первой единицей в последовательности стоит не «-1», то идти на Выход с сообщением «n - составное».
2. Идти на Выход с сообщением «n – простое с вероятностью ε^t ».
Выход.

Обратим внимание на то, что в последовательности b_0, b_1,…, b_s каждый последующий член является квадратом предыдущего по модулю n, а последний член есть ни что иное как a^{n-1} mod n.

Вероятность ошибки теста на одной итерации составляет $\varepsilon \leq \frac{(n)}{4n}$, то есть верхняя граница ошибки на одной итерации для теста Миллера-Рабина в 2 раза меньше аналогичной для теста Соловея-Штрассена и в 4 раза – для теста Ферма.
Пример использования теста Миллера-Рабина:
n=65=64+1=2^6+1. r=1, s=6. t=5.
1. 1-я итерация:
1.1. a=8.
1.2. Составляем последовательность: b_0=8, b_1=64=-1, b_2=1, b_3=1, b_4=1, b_5=1, b_6=1.
1.3. В последовательности встретилась «1».
1.4. Перед первой единицей стоит «—1».
1. 2-я итерация:
1.1. a=11.
1.2. Составляем последовательность: b_0=11, b_1=56, b_2=16, b_3=61, b_4=16, b_5=61, b_6=16.
1.3. В последовательности не встретилась «1».
Выход: « n - составное число».

Задания к разделу.

1) Реализовать процедуру генерации простых чисел методом случайного поиска среди 128-битных чисел, старший бит которых равен 1 и проверки

а) тестом Ферма

б) тестом Соловея-Штрассена

в) тестом Миллера-Рабина.

Количество итераций вероятностного теста должно быть таково, чтобы вероятность ошибки не превышала 0,1. Вероятность ошибки определяется исходя из оценки ε для теста. Количество итераций для теста Ферма задать равным 50.
2) Получить с помощью этой процедуры 10 простых чисел. Для каждого эксперимента найти количество перебранных чисел до получения простого. Результаты оформить в виде таблицы.

№	*1*	*2*	*…*	*10*
p				
n				

Здесь №-номер эксперимента, p – найденное простое число, n –количество перебранных чисел до получения простого.

3) Рассчитать k – ожидаемое количество перебранных чисел до получения простого числа, исходя из асимптотического закона.

Данные для самопроверки к разделу.

Данными следует пользоваться следующим образом:

· Задать значение параметра надежности теста t=1.

· Подставить в качестве входного параметра n число из колонки «Числа для проверки».

· Несколько (10-20) раз «прогнать» программу с заданными входными параметрами.

· Выводы о корректности реализованного теста следует делать на основании сравнения результата теста с данными из таблицы (колонка «Результат теста»).

Тип числа	**Числа для проверки**		**Результат теста**
Простые числа	**0 8363**	**0 1867**	**Всегда «простое»**
	0 1657	**0 1901**	
	0 9781	**0 1303**	
	0 9049	**0 5479**	
	0 6673	**0 8111**	
Числа Кармайкла	**0 1105**	**0 8911**	**Для теста Ферма – всегда «простое», для тестов Миллера-Рабина и Соловея-Штрассена – чаще «составное», чем «простое»**
	0 2465	**0 6601**	
	0 10585	**0 2821**	
	0 1729	**0 15841**	
	0 2821	**0 52633**	
Составные, нечетные, не являющиеся числами Кармайкла	**0 625**	**0 1969**	**Чаще «составное», чем «простое»**
	0 791	**0 5705**	
	0 3871	**0 3445**	
	0 2007	**0 6105**	
	0 6785	**0 3621**	

2. Вопросы к коллоквиуму.

Вопросы к коллоквиуму совпадают с вопросами к экзамену, приведенными ниже и выбранными в соответствии с модулем, в котором проводится коллоквиум.

3. Примерные темы докладов:

1. Криптография в Древнем мире.
2. Исторические методы стеганографии.
3. Криптография в Средние века и в Новое время.
4. Дисковые шифраторы.
5. Криптография на рубеже 19-20 вв.
6. История отечественной криптографии.
7. Шифрование аналогового сигнала.
8. Клод Шеннон и его вклад в криптографию.
9. Алан Тьюринг и его вклад в криптографию.
10. Лауреаты премии Алана Тьюринга.
11. Первый блочный шифр – Lucifer.

12. Современная стеганография – математические методы.
13. Электронные водяные знаки.
14. Ади Шамир и его вклад в криптографию.
15. Шифрование и аутентификация в современных беспроводных сетях связи.
16. Парольные схемы аутентификации.
17. Одноразовые пароли.
18. Протоколы с нулевым разглашением.
19. Финалист конкурса NIST AES блочный шифр Serpent.
20. Финалист конкурса NIST AES блочный шифр Twofish.
21. Финалист конкурса NIST AES блочный шифр RC6.
22. Финалист конкурса NIST AES блочный шифр MARS.
23. Первый блочный шифр Lucifer и его криптоанализ.
24. Победитель конкурса eStream поточный шифр HC-128.
25. Победитель конкурса eStream поточный шифр Rabbit.
26. Победитель конкурса eStream поточный шифр Salsa 20/12.
27. Победитель конкурса eStream поточный шифр SOSEMANUK.
28. Победитель конкурса eStream поточный шифр Grain.
29. Победитель конкурса eStream поточный шифр Mickey.
30. Блочный шифр Camellia и область его применения.
31. Шифр Blowfish и область его применения.
32. Шифр CAST и область его применения.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Введение в криптографию.	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
2.	История криптографии. Исторические шифры.	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
3.	Математическая модель шифра. Теория секретности Шеннона	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
4.	Блочные шифры	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
5.	Псевдослучайные последовательности и поточные шифры.	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.

6.	Теория имитостойкости Симмонса и криптографические хэш-функции.	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
7.	Асимметричные (с открытым ключом) шифры	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
8.	Схемы цифровой подписи.	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
9.	Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
10.	Введение в криптографические протоколы	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.

Порядок выполнения каждого вида самостоятельной работы:

Для подготовки к собеседованиям и коллоквиумам необходимо пользоваться конспектом лекций и [1] из списка основной литературы. Для выполнения расчетных работ на практических занятиях с разделением на подгруппы следует использовать [1] из дополнительной литературы, методички и раздаточный материал, выдаваемые преподавателем и хранящиеся на кафедре информационной безопасности. Для получения расширенных и углубленных знаний по тематике рекомендуется пользоваться ссылками из списка интернет-ресурсов, приведенных в данном УМК, а также электронными и бумажными номерами научных журналов, имеющихся в ИБЦ, областной научной библиотеке и сети интернет. Особенное внимание рекомендуется обратить на издания «Математические вопросы криптографии», «Прикладная дискретная математика», материалами конференций RealWorldCrypto, Crypto, Eurocrypt, Ruscrypt, Sibecrypt, Asiacrypt.

Контроль за самостоятельной работой осуществляется на коллоквиуме

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения экзамена – комплект экзаменационных билетов

Вопросы к экзамену

1. Основные понятия и определения криптографии.
2. Виды криптосистем. Задачи, решаемые методами криптографии.
3. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.
4. История криптографии. Основные этапы становления науки криптографии.
5. Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски
6. Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ.
7. Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу.
8. Композиции шифров. Enigma. Шифр Хейглина.
9. Математическая модель шифра.
10. Атаки и угрозы шифрам.
11. Блочные шифры и их ключевая система. Замены и перестановки. S-P-сеть.
12. Сеть Файстеля. Шифр ГОСТ 28147-89.
13. Конечные кольца и поля многочленов.
14. Шифр SQUARE.
15. Шифр AES
16. Режимы шифрования.
17. Многократное шифрование. Композиция блочных шифров.
18. Совершенные шифры. Пример совершенного шифра.
19. Энтропийные характеристики шифров. Идеальные шифры.
20. Избыточность языка.
21. Оценка числа ложных ключей и расстояние единственности.
22. Безусловно стойкие и вычислительно стойкие шифры.
23. Псевдослучайные последовательности (ПСП). Характеристики генераторов ПСП (ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ.
24. Поточные шифры. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры.
25. Регистры сдвига с обратной линейной связью (РСЛОС).
26. ПСГ на основе РСЛОС.
27. Шифр Trivium.
28. Нелинейные регистры сдвига.
29. Шифр RC4.
30. Теория имитостойкости Симмонса. Имитация и подмена сообщения. Характеристики имитостойкости. Совершенная имитостойкость.

31. Коды аутентификации сообщений.
32. Защитные контрольные суммы.
33. Криптографические хэш-функции и требования к ним.
34. Подходы к проектированию хэш-функций.
35. Хэш-функции на основе блочного шифра.
36. Схема Меркла-Дамгарда и ГОСТ Р 34.11-2012.
37. Схема «губка» и SHA-3.
38. Коды аутентификации сообщений.
39. Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях.
40. Криптосистема Диффи-Хэллмана. Пример.
41. Криптосистема RSA. Пример.
42. Криптосистема Эль-Гамаля. Пример.
43. Криптосистема Рабина. Пример.
44. Криптосистема Гольдвассер-Микали. Пример.
45. Криптосистема Блюма-Гольдвассер. Пример.
46. Рюкзачные шифры. Криптосистема Меркла-Хэллмана.
47. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.
48. Подпись RSA, Эль-Гамаля.
49. Подпись Фиата-Шамира.
50. Подпись Онга-Шнорра-Шамира.
51. Неотрицаемая подпись Шаума-ван-Антверпена.
52. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.
53. Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка.
54. Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра (ЭЦП) в Zp к шифру (ЭЦП) на эллиптической кривой.
55. Шифр Эль-Гамаля на эллиптической кривой.
56. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001 (2012), ECDSA

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОК-8 - способность к самоорганизации и самообразованию	знать: - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; уметь: - самостоятельно строить процесс овладения информацией, отобранной и	Практические работы на занятиях с разделением на подгруппы, доклады, коллоквиум, экзаменационный билет	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и

		структурированной для выполнения профессиональной деятельности.		правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-5 - способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	знать: - внутреннюю структуру криптографических алгоритмов, их область применения и свойства; внутреннее содержание отечественных криптографических стандартов, их характеристики по сравнению с зарубежными. уметь: - самостоятельно реализовать стандартный криптографический алгоритм; применять на практике отечественные стандарт.	Практические работы на занятиях с разделением на подгруппы, доклады, коллоквиум, экзаменационный билет	
3.	ПК-10 - способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	знать: - основы теорий секретности и имитостойкости, тесты на простоту, общие приемы дифференциального и линейного криптоанализа, основные алгоритмы факторизации и дискретного логарифмирования. Математические модели и свойства криптосистем. уметь: - показать полноту и корректность криптосистемы, получать криптографические ключи, построить математическую модель и вычислить вероятностные характеристики криптосистемы.	Практические работы на занятиях с разделением на подгруппы, доклады, коллоквиум, экзаменационный билет	

* - не предусмотрен

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. 1. Крамаров С.О. Криптографическая защита информации: учеб. пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — М.: РИОР: ИНФРА-М, 2018. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6 [Электронный ресурс]. - URL: http://znanium.com/catalog/product/901659 (дата обращения: 15.05.2020).

7.2. Дополнительная литература:

2. 1. Бабаш А.В. Криптографические методы защиты информации. Том 3: Учебнометодическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.: 60x88 1/8. - (Высшее образование: Бакалавриат). ISBN 978-5-369- 01304-5. [Электронный ресурс]. – URL: http://znanium.com/catalog/product/432654 (дата обращения: 15.05.2020).
3. 2. Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97571.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

7.3. Интернет-ресурсы

- вузовские электронно-библиотечные системы учебной литературы.
- доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru
- A. Menezes, P. van Oorschort, S. Vanstone, Handbook of Applied Cryptography – CRC Press Inc., 5th Printing, 2001 [On-line] http://www.cacr.uwaterloo.ca/hac/
- http://www.ietf.org/rfc.html [On-line] - документы IETF – инженерного совета Интернета
- http://www.iacr.org/

7.4 Современные профессиональные базы данных и информационные справочные системы:

- базы данных, содержащие материалы по специфике дисциплины, из перечня Баз данных, Реестра учебного ПО 2020 и Электронных ресурсов, выставленных на сайте https://www.utmn.ru/obrazovanie/normativnye-dokumenty/akkteditatsiya/dokumenty-tyumgu/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- платформа для электронного обучения Microsoft Teams.
- Visual Studio или другая IDE

9. **Технические средства и материально-техническое обеспечение дисциплины (модуля)**

Компьютерный класс

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020г.

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ
Рабочая программа
для обучающихся по направлению подготовки
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Атманских М.Б., Ниссенбаум О.В. Криптографические протоколы. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Криптографические методы защиты информации [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Атманских М.Б., Ниссенбаум О. В. 2020.

1. Пояснительная записка

Студент приобретет теоретические знания об использовании криптографических протоколов для защиты информации и об их уязвимостях; практическое освоение приемов и методов программной реализации криптографических протоколов; владение основами алгоритмизации и автоматизации выполнения работ. В ходе выполнения практических работ на занятиях с разделением на подгруппы научится корректно применять современные защищенные информационные технологии.

Программа дисциплины ориентирована на достижение следующих целей: · приобретение основополагающих знаний о подходах к анализу и синтезу криптографических протоколов с государственными и международными стандартами в этой области; овладение навыками корректного применения современных защищенных информационных технологий; · воспитание ответственности к профессиональной деятельности, воспитание самообразования; · развитие навыков программной реализации криптографических протоколов; · формирование готовности использовать приобретенные знания в профессиональной деятельности.

Исходя из целей, в программе дисциплины «Криптографические протоколы» предусматриваются задачи: · сформировать у обучающегося необходимый объем знаний об основных механизмах функционирования протоколов, применяемых для обеспечения того или иного свойства безопасности; · научить корректно применять современные защищенные информационные технологии; · развить навыки программной реализации криптографических протоколов; · сформировать умения применять знания о свойствах, характеризующих защищенность криптографических протоколов на практике.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Алгебра и математическая логика», «Языки программирования», «Информатика», «Дискретная математика и исследование операций», «Теоретико-числовые методы в криптографии», «Криптографические методы защиты информации».

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*) УП компетенции

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-8 - способность к самоорганизации и самообразованию		знать: - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; уметь: - самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности.
ПК-8 - способность участвовать в разработке		знать: - основы Интернет-технологий; средства и методы

подсистемы информационной безопасности компьютерной системы		хранения и передачи аутентификационной информации; основные протоколы идентификации и аутентификации абонентов сети. уметь: - формализовать поставленную задачу; разрабатывать эффективные алгоритмы и программы; корректно применять симметричные и асимметричные криптографические алгоритмы.
ПК-18 - способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		знать: - средства и методы хранения и передачи аутентификационной информации; основные протоколы идентификации и аутентификации абонентов сети; основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; криптографические стандарты; алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах. уметь: - разрабатывать эффективные алгоритмы и программы; корректно применять симметричные и асимметричные криптографические алгоритмы; проводить оценку сложности алгоритмов.

* не предусмотрено

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		6 семестр
Общий объем зач. ед.	3	3
час.	108	108
Из них:		
Часы аудиторной работы (всего):	72	72
Лекции	36	36
Практические занятия		
Лабораторные/практические занятия по подгруппам	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	36	36

Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной) и традиционной систем оценок.

Оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических работ на занятиях с разделением на подгруппы. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 100 баллов – зачтено.

Оценка «зачтено» ставится, если студент набрал 61 балл или выше. Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать зачет.

Оценка студента на зачете в рамках традиционной системы оценок выставляется на основе ответа студента на теоретические вопросы. Эта оценка характеризует уровень знаний, умений и навыков, приобретенных студентом в ходе изучения дисциплины.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса и практическое задание из пройденных тем на усмотрение преподавателя. Для получения оценки «зачтено» студентом должно быть сдано минимум 5 практических работ на занятиях с разделением на подгруппы и сделан ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности.

Примечание. Студент, желающий исправить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу зачета.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Основные понятия.	8	4	0	4	0
2.	Привязка к биту и электронная жеребьевка.	4	2	0	2	0
3.	Разделение секрета.	8	4	0	4	0
4.	Идентификация и аутентификация	8	4	0	4	0

5.	Протоколы идентификации с нулевым разглашением.	8	4	0	4	0
6.	Протоколы открытых сделок	8	4	0	4	0
7.	Инфраструктура открытых ключей.	8	4	0	4	0
8.	Управление ключами.	8	4	0	4	0
9.	Прикладные протоколы.	12	6	0	6	0
	Итого (часов)	108	36	0	36	0

4.2. Содержание дисциплины (*модуля*) по темам

Модуль 1. Примитивные протоколы.

1. Основные понятия. Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Понятие криптографического протокола. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей. Подходы к классификации криптографических протоколов. Подходы к моделированию криптографических протоколов. Понятие уязвимости и атаки на криптографический протокол. Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры. Основные подходы к автоматизации анализа протоколов

2. Привязка к биту и электронная жеребьевка. Вычислительная и безусловная связанность, секретность. Блоб. Протоколы привязки к биту на основе проблемы дискретного логарифмирования, на основе симметричной криптосистемы, на основе односторонней функции, односторонней перестановки.

3. Разделение секрета. Понятие схемы разделения секрета (СРС). Группа доступа. Структура доступа. Пороговые СРС – схема Шамира, схема Блекли, схема на основе Китайской теоремы об остатках. Разделение секрета для произвольной группы доступа. Совершенная СРС. Идеальное разделение секрета. Проверяемое разделение секрета. Протоколы конфиденциальных вычислений. Пример для схемы Шамира.

Модуль 2. Идентификация и сделки.

4. Идентификация и аутентификация. Понятие об идентификации. Классификация схем идентификации и аутентификации. Парольные схемы. Разновидности парольных схем. Требования к парольным схемам. Использование хэш-функций в парольных 9 схемах. Одноразовые пароли. Схема Лампорта. Протоколы рукопожатия. Требования к протоколам рукопожатия. Область применения протоколов рукопожатия.

5. Протоколы идентификации с нулевым разглашением. Понятие об интерактивных системах доказательства (ИСД). Примеры ИСД (квадратичные невычеты; неизоморфизм графов). Примеры ИСД с нулевым разглашением (изоморфизм графов). Вопросы реализации ИСД. Нулевое разглашение при параллельной композиции раундов. Схема Фиата-Шамира. Схема Файге-Фиата-Шамира. Схема Шнорра. Схема Брикелла-МакКарли. Схема Окамото и теорема о ее условной стойкости. Схема ГиллуКискатр. Доказательства полноты и корректности этих схем.

6. Протоколы открытых сделок. Слепая подпись. Затемненная подпись. Применение слепых подписей. Скрытый канал. Подписи со скрытым каналом. Скрытый канал на основе подписи Онга-Шнорра-Шамира. Подход к построению скрытого канала. Подписи, свободные от скрытого канала. Покер по телефону. Электронная монета и электронные платежи. Протоколы голосования. Протоколы установления подлинности.

Модуль 3. Управление ключами и прикладные протоколы.

7. Инфраструктура открытых ключей. Управление открытыми ключами. Основы организации и основные компоненты инфраструктуры открытых ключей. Сертификат открытого ключа. Стандарт X.509. Сервисы инфраструктуры открытых ключей. Удостоверяющий центр. Центр регистрации. Репозиторий. Архив сертификатов. Конечные субъекты. Архитектуры инфраструктуры открытых ключей. Проверка и отзыв сертификата открытого ключа.
8. Управление ключами. Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами. Централизованная выработка ключа. Совместная выработка ключа. Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра. Схемы Wide-Mouth Frog, Yahalom, протокол Нидхема-Шредера, Отвея-Рииса. Бесключевой протокол Шамира. Протокол Диффи-Хэллмана. Протокол Нидхема-Шредера на основе шифра с открытым ключом. Широковещательное распределение ключей. Протокол Kerberos.
9. Прикладные протоколы. Построение семейства протоколов KriptoKnight на основе базовых протоколов взаимной аутентификации и распределения ключей. Особенности построения семейства протоколов IPsec. Протоколы Oakley, ISAKMP, IKE. Протоколы SKIP, SSL/TLS и особенности их реализации.

Темы практических работ на занятиях с разделением на подгруппы

Модуль 1. Примитивные протоколы.
Тема 1: Основные понятия.
1. Анализ безопасности простейших протоколов. Классификация атак.
2. Анализ протоколов цифровых подписей. Анализ DSA и ГОСТ.
Тема 2: Привязка к биту и электронная жеребьевка.
3. Компьютерная реализация схем электронной жеребьевки и привязки к биту.
Тема 3: Разделение секрета.
4. Реализация пороговых схем разделения секрета и СРС для произвольной структуры доступа.
5. Проверяемое разделение секрета и конфиденциальные вычисления.
Модуль 2. Идентификация и сделки.
Тема 4: Идентификация и аутентификация.
6. Парольные схемы. Одноразовые пароли.
7. Схемы рукопожатия.
Тема 5: Протоколы идентификации с нулевым разглашением.
8. Интерактивные системы доказательства.
9. Имитационное моделирование протоколов идентификации на основе ИСД с нулевым разглашением.
Тема 6: Протоколы открытых сделок.
10. Компьютерная реализация схем слепой подписи и скрытого канала. Компьютерная реализация протокола «Покер по телефону» для 3-х игроков.
11. Имитационное моделирование схемы электронных денег с монетами одинакового достоинства.
Модуль 3. Управление ключами и прикладные протоколы.
Тема 7: Инфраструктура открытых ключей.
12. Изучение работы с удостоверяющим центром при помощи CryptoPro.
13. Формирование и проверка сертификата с использованием CryptoPro.
Тема 8: Управление ключами.
14. Компьютерная реализация протокола передачи секретного ключа через доверенный центр (работа в группах).

15. Компьютерная реализация протокола передачи секретного ключа средствами асимметричной криптографии(работа в группах).
Тема 9: Прикладные протоколы.
16. Протоколы семейства KriptoKnight для различных сетевых конфигураций и условий применения.
17. Протоколы семейства IPSec.
18. Протоколы семейства SSL/TLS.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Основные понятия.	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
2.	Привязка к биту и электронная жеребьевка.	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
3.	Разделение секрета.	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
4.	Идентификация и аутентификация.	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
5.	Протоколы идентификации с нулевым разглашением .	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
6.	Протоколы открытых сделок.	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
7.	Инфраструктура открытых ключей.	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.
8.	Управление ключами	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с

		учебной литературой. Подготовка к коллоквиуму.
9.	Прикладные протоколы.	Конспектирование материала на лекционных занятиях. Выполнение практической работы на занятиях с разделением на подгруппы. Работа с учебной литературой. Подготовка к коллоквиуму.

Порядок выполнения каждого вида самостоятельной работы:

Для подготовки к собеседованиям и коллоквиумам необходимо пользоваться конспектом лекций и [1] из списка основной литературы. Для выполнения расчетных работ на практических занятиях с разделением на подгруппы следует использовать [1] из дополнительной литературы, методички и раздаточный материал, выдаваемые преподавателем и хранящиеся на кафедре информационной безопасности. Для получения расширенных и углубленных знаний по тематике рекомендуется пользоваться ссылками из списка интернет-ресурсов, приведенных в данном УМК, а также электронными и бумажными номерами научных журналов, имеющихся в ИБЦ, областной научной библиотеке и сети интернет. Особенное внимание рекомендуется обратить на издания «Математические вопросы криптографии», «Прикладная дискретная математика», материалами конференций RealWorldCrypto, Crypto, Eurocrypt, Ruscrypt, Sibecrypt, Asiacrypt.

Контроль за самостоятельной работой осуществляется на коллоквиуме.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения зачета – комплект заданий для зачета

Вопросы к зачету

1. Понятие о криптографических протоколах. Основные виды протоколов. Примитивные и прикладные протоколы.

2. Понятие о криптографических протоколах. Полнота и корректность.

3. Протоколы подбрасывания монеты. Применение протоколов подбрасывания монеты для выработки сеансовых ключей.

4. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной связанностью.

5. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной секретностью.

6. Протоколы привязки к биту. Блоб.

7. Понятие о разделении секрета. Группа доступа, структура доступа. Требования к ним. Минимальная группа доступа.

8. Совершенная СРС (система разделения доступа), идеальная СРС.

9. Пороговые схемы разделения секрета. Схема Шамира, ее совершенность и идеальность.
10. Схема Блэкли. Вопрос о ее совершенности и идеальности.

11. СРС на основе Китайской теоремы об остатках. Вопрос о ее совершенности и идеальности.

12. СРС для произвольной структуры доступа. Вопрос о ее совершенности и идеальности.
13. Протоколы конфиденциальных вычислений.

14. Проверяемое разделение секрета.

15. Протоколы идентификации. Классификация. Требования.

16. Парольные схемы. Разновидности. Область применения.

17. Интерактивные системы доказательств. Полнота, корректность. Пример интерактивной системы доказательств для языка «Квадратичные невычеты».

18. Доказательства с нулевым разглашением. Статистическая неразличимость, вероятностная неразличимость. Пример интерактивного доказательства с нулевым разглашением для языка «Изоморфизм графов».

19. Протоколы идентификации на основе теории ИСД с нулевым разглашением. Схема Фиата-Шамира. Схема Файге-Фиата-Шамира. Их полнота и корректность.

20. Схема идентификации Шнорра. Схема Брикелла-МакКарли. Их полнота и корректность.

21. Схема идентификации Окамото и теорема о ее условной стойкости.

22. Схема Гиллу-Кискатр. Ее полнота и корректность.

23. Слепая подпись.

24. Скрытый канал.

25. Протокол «Покер по телефону».

26. Электронная монета. Электронные деньги. Требования к схемам электронных денег. Схема электронного кошелька с банкнотами одного достоинства.

27. Электронная монета. Электронные деньги. Требования к схемам электронных денег. Разного достоинства. Схема с копилкой.

28. Протоколы голосования.

29. Протоколы установления подлинности.

30. Управление ключами. Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами.

31. Централизованная выработка ключа. Совместная выработка ключа. Требования к секретному ключу. Алгоритм фон Неймана.

32. Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра.

33. Схемы Wide-Mouth Frog, Yahalom. Их анализ.

34. Протокол Нидхема-Шредера. Его анализ.

35. Протокол Отвея-Рииса. Его анализ.

36. Бесключевой протокол Шамира и атака «Человек посередине».

37. Протокол Диффи-Хэллмана и атака «Человек посередине». Противодействие этой атаке. 38. Протокол Нидхема-Шредера на основе шифра с открытым ключом. 39. Широковещательное распределение ключей.

40. Стандарт x.509.

41. Инфраструктура открытых ключей. Сертификаты и справочники открытых ключей. Многоуровневая система удостоверяющих центров.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (из паспорта компетенций)*	Оценочные материалы	Критерии оценивания
1.	ОК-8 - способность к самоорганизации и самообразованию	знать: - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; уметь: - самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности.	Практические работы на занятиях с разделением на подгруппы, коллоквиум, задания для зачета	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле

2.	ПК-8 - способность участвовать в разработке подсистемы информационной безопасности компьютерной системы	знать: - основы Интернет-технологий; средства и методы хранения и передачи аутентификационной информации; основные протоколы идентификации и аутентификации абонентов сети. уметь: - формализовать поставленную задачу; разрабатывать эффективные алгоритмы и программы; корректно применять симметричные и асимметричные криптографические алгоритмы.	Практические работы на занятиях с разделением на подгруппы, коллоквиум, задания для зачета	успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
3.	ПК-18 - способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства	знать: - средства и методы хранения и передачи аутентификационной информации; основные протоколы идентификации и аутентификации абонентов сети; основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; криптографические стандарты; уметь: корректно применять симметричные и асимметричные криптографические алгоритмы; проводить оценку сложности алгоритмов.	Практические работы на занятиях с разделением на подгруппы, коллоквиум, задания для зачета	

	криптографической защиты информации			

* - не предусмотрен

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Криптографическая защита информации: учеб. пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — М.: РИОР: ИНФРА-М, 2018. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. URL: http://znanium.com/catalog/product/901659 (дата обращения: 15.05.2020). - Режим доступа: по подписке.

7.2. Дополнительная литература:

1. Бабаш А.В. Криптографические методы защиты информации. Том 3: Учебнометодическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.: 60x88 1/8. - (Высшее образование: Бакалавриат). ISBN 978-5-369-01304-5. [Электронный ресурс]. – URL: http://znanium.com/catalog/product/432654 (дата обращения: 15.05.2020). - Режим доступа: по подписке.
2. Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97571.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

7.3. Интернет-ресурсы

- вузовские электронно-библиотечные системы учебной литературы.
- доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru
- A. Menezes, P. van Oorschort, S. Vanstone, Handbook of Applied Cryptography – CRC Press Inc., 5th Printing, 2001 [On-line] http://www.cacr.uwaterloo.ca/hac/
- http://www.ietf.org/rfc.html [On-line] - документы IETF – инженерного совета Интернета
- http://www.iacr.org/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- платформа для электронного обучения Microsoft Teams.
- Visual Studio или другая IDE

9. **Технические средства и материально-техническое обеспечение дисциплины (модуля)**

Компьютерный класс.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Паюсова Т.И. Модели безопасности компьютерных систем. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Модели безопасности компьютерных систем [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Паюсова Т.И., 2020.

1. Пояснительная записка

Основной целью дисциплины «Модели безопасности компьютерных систем» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой информации; обучение общим принципам построения моделей безопасности и политик безопасности, основным методам исследования корректности систем защиты, методологии обследования и проектирования систем защиты.

Задачи дисциплины «Модели безопасности компьютерных систем»:

· изложение теоретических основ компьютерной безопасности;

· описание моделей безопасности информационных систем;

· описание моделей доступа в информационных системах;

· обучение методологии обследования и проектирования систем защиты;

· обучение навыкам настройки основных компонентов систем защиты и применения технологий защиты.

В результате освоения дисциплины у студентов будут сформированы следующие компетенции:

ОК-7 - способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности;

ОПК-10 - способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах;

ОПК-2 - способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов;

ОПК-4 - способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

ОПК-9 - способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации;

ПК-1 - способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности;

ПК-2 - способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований;

ПК-4 - способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Защита операционных систем», «Криптографические протоколы», «Криптографические методы защиты информации», «Основы информационной безопасности».

Дисциплина «Модели безопасности компьютерных систем» способствует освоению следующих дисциплин: «Разработка и защита медицинских информационных систем», «Анализ и управление рисками информационной безопасности».

1.2.**Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)**

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-7 - способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности		Знать: основные модели доступа в информационной системе. Уметь: реализовывать основные модели доступа в информационной системе.
ОПК-10 - способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах		Знать: методы формального описания модели злоумышленника. Уметь: формально описывать модель злоумышленника.
ОПК-2 - способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов		Знать: основные способы формального описания и анализа политик безопасности. Уметь: формально описывать и анализировать политику безопасности.
ОПК-4 - способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами		Знать: методы анализа модели угроз. Уметь: анализировать модель угроз.
ОПК-9 - способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными		Знать: основные модели доступа в информационной системе. Уметь: реализовывать основные модели доступа в информационной системе.

потоками в компьютерных системах с учетом угроз безопасности информации		
ПК-1 - способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности		Знать: методы формального описания модели злоумышленника. Уметь: формально описывать модель злоумышленника.
ПК-2 - способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований		Знать: основные способы формального описания и анализа политик безопасности. Уметь: формально описывать и анализировать политику безопасности.
ПК-4 - способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем		Знать: методы анализа модели угроз. Уметь: анализировать модель угроз.

* не предусмотрено

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		8 семестр
Общий объем зач. ед.	3	3
час.	108	108
Из них:		
Часы аудиторной работы (всего):	72	72
Лекции	36	36
Практические занятия	36	36

Лабораторные/практические занятия по подгруппам	0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	36	36
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет

3. Система оценивания

3.1. Для текущего контроля применяется 100-балльная система оценивания. Баллы проставляются за посещение практических занятий, а также активную работу на них. Результаты текущего контроля учитываются при промежуточной аттестации. Перевод баллов в зачет осуществляется по следующей шкале: от 61 до 100 баллов – «зачтено». Зачет проходит в устной форме, по билетам. В билете – 2 вопроса. Для получения оценки «зачтено» ответ студента должен показывать, что студент знает и понимает смысл и суть описываемой темы, ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Ответ может содержать небольшие недочеты.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные/практические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Введение в теоретический подход к обеспечению информационной безопасности.	8	4	4	0	0
2.	Математические основы построения моделей безопасности.	8	4	4	0	0
3.	Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана	8	4	4	0	0
4.	Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД).	8	4	4	0	0

5.	Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant.	8	4	4	0	0
6.	Модели компьютерных систем с мандатным управлением. Модель Белла-ЛаПадулы.	8	4	4	0	0
7.	Модели компьютерных систем с мандатным управлением. Модель Биба. Модель систем военных сообщений.	8	4	4	0	0
8.	Модели компьютерных систем с ролевым управлением	8	4	4	0	0
9.	Модели безопасности информационных потоков и изолированной программной среды.	8	4	4	0	0
	Итого (часов)	108	36	36	0	0

4.2. Содержание дисциплины (*модуля*) по темам

Модуль 1. Формальное обоснование информационной безопасности информационных систем.

1. Введение в теоретический подход к обеспечению информационной безопасности. Основные понятия защиты информации (субъекты, объекты, доступ, граф доступов, информационные потоки). Постановка задачи построения защищенной автоматизированной системы (АС). Ценность информации.

2. Математические основы построения моделей безопасности. Применение теории графов и теории автоматов для обеспечения информационной безопасности информационных систем. Понятие автомата, графа, математической решѐтки. Алгоритмически разрешимые и алгоритмически неразрешимые проблемы. Проблема адекватности реализации модели безопасности в реальной компьютерной системе.

3. Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU). Определение дискреционного контроля доступа. Принципы построения матрицы доступов. Контроль над процессом передачи прав доступа в системе. Модель системы безопасности Харрисона-РуззоУльмана (HRU). Основные положения модели. Теорема об алгоритмической неразрешимости задачи проверки безопасности произвольной системы HRU

Модуль 2. Дискреционная и мандатная модели разграничения прав доступа в информационной системе.

4. Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД). Модель типизированной матрицы доступов. Основные положения модели. Теорема о существовании алгоритма проверки безопасности ациклических систем монотонных ТМД.

5. Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant. Модель распространения прав доступа Take-Grant. Теоремы о передаче прав в графе доступов, состоящем из субъектов, и произвольном графе доступов.

Расширенная модель Take-Grant и ее применение для анализа информационных потоков в АС.
6. Модели компьютерных систем с мандатным управлением. Модель Белла-ЛаПадулы. Модель Белла-Лападулы как основа построения систем мандатного разграничения доступа. Основные положения модели. Базовая теорема безопасности (BST). Политика low-watermark в модели Белла-ЛаПадулы.
Модуль 3. Модели безопасности информационных потоков и изолированной программной среды. Ролевая модель доступа.
7. Модели компьютерных систем с мандатным управлением. Модель Биба. Модель систем военных сообщений. Применение модели Биба для реализации мандатной политики целостности. Применение модели систем военных сообщений для систем приема, передачи и обработки почтовых сообщений, реализующих мандатную 8 политику безопасности. Шесть теоретических принципов политики контроля целостности. Соответствие правил модели Кларка-Вилсона принципам политики целостности.
8. Модели компьютерных систем с ролевым управлением. Понятие ролевого управления доступом. Базовая модель ролевого управления доступом. Понятие администрирования ролевого управления доступом. Администрирование иерархии ролей. Понятие мандатного ролевого управления доступом. Требования либерального мандатного управления доступом.
9. Модели безопасности информационных потоков и изолированной программной среды. Автоматная модель безопасности информационных потоков. Вероятностная модель безопасности информационных потоков. Информационное невлияние. Информационное невлияние с учетом фактора времени. Монитор безопасности объектов. Монитор безопасности субъектов. Теоремы о достаточных условиях гарантированного выполнения политики безопасности в компьютерных системах. Базовая теорема изолированной программной среды.

Планы практических занятий.
Модуль 1. Формальное обоснование информационной безопасности информационных систем.
1) Математические основы построения моделей безопасности. Построение модели безопасности информационной системы с помощью теории автоматов и теории графов.
2) Математические основы построения моделей безопасности. Построение модели безопасности информационной системы с помощью теории графов.
3) Математические основы построения моделей безопасности. Построение модели безопасности информационной системы с помощью вероятностного подхода.
Модуль 2. Дискреционная и мандатная модели разграничения прав доступа в информационной системе.
4) Дискреционная модель доступа. Реализация дискреционной модели безопасности (модель Харрисона-Руззо-Ульмана).
5) Дискреционная модель доступа. Реализация дискреционной модели доступа (модель Take-Grant).
6) Мандатная модель доступа. Реализация мандатной модели доступа (модель Белла-Лападулы).
Модуль 3. Модели безопасности информационных потоков и изолированной программной среды. Ролевая модель доступа.
7) Ролевая модель доступа. Реализация ролевой модели разграничения прав доступа (RBAC). Реализация администрирования иерархии ролей.

8) Атрибутивная модель доступа. Реализация атрибутивной модели доступа. Сравнительный анализ атрибутивной и ролевой моделей доступа.
9) Модели безопасности информационных потоков и изолированной программной среды. Сравнительный анализ модели безопасности информационных потоков и изолированной программной среды.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Введение в теоретический подход к обеспечению информационной безопасности	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение расчетной работы, подготовка к ответам на вопросы к практическому заданию и к собеседованию.
2.	Математические основы построения моделей безопасности	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение расчетной работы, подготовка к ответам на вопросы к практическому заданию и к собеседованию.
3.	Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU)	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение расчетной работы, подготовка к ответам на вопросы к практическому заданию и к собеседованию.
4.	Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД)	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение расчетной работы, подготовка к ответам на вопросы к практическому заданию и к собеседованию.
5.	Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа TakeGrant	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение расчетной работы, подготовка к ответам на вопросы к практическому заданию и к собеседованию.
6.	Модели компьютерных систем с мандатным управлением. Модель БеллаЛаПадулы	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение расчетной работы, подготовка к ответам на вопросы к практическому заданию и к собеседованию.
7.	Модели компьютерных систем с мандатным управлением. Модель Биба. Модель систем военных сообщений	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение расчетной работы, подготовка к ответам на

		вопросы к практическому заданию и к собеседованию.
8.	Модели компьютерных систем с ролевым управлением	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение расчетной работы, подготовка к ответам на вопросы к практическому заданию и к собеседованию.
9.	Модели безопасности информационных потоков и изолированной программной среды	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение расчетной работы, подготовка к ответам на вопросы к практическому заданию и к собеседованию.

Порядок выполнения каждого вида самостоятельной работы:

1. Конспектирование и проработка лекционного материала.
2. Работа с основной и дополнительной литературой.
3. Анализ и проработка результатов практического занятия.
4. Подготовка доклада.

Контроль за самостоятельной работой осуществляется во время лекционных и практических занятий, а также во время финального испытания (зачет).

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения зачета – контрольная работа.

Пример варианта контрольной работы:

Вариант 1. Тестовая часть:

Вопрос 1. Выберите корректные утверждения из нижеприведенного списка:

1. Контейнеры могут состоять из объектов или других контейнеров;
2. Контейнеры могут состоять из субъектов или других контейнеров;
3. Контейнеры могут состоять из субъектов, объектов или других контейнеров;
4. Субъекты могут получать доступ к объектам целиком, но не к их части;
5. Объекты могут получать доступ к субъектам целиком, но не к их части;
6. Объекты могут получать доступ к контейнеру и сущностям, из которых он состоит;
7. Объекты могут получать доступ к контейнеру и субъектам, из которых он состоит.

Вопрос 2. Каким из нижеприведенных требований должна соответствовать математическая решетка?

1. Наличие отношения частичного порядка;
2. Наличие отношения строгого порядка;
3. Наличие наибольшей верхней границы;
4. Наличие наименьшей верхней границы;
5. Отсутствие наибольшей верхней границы;

6. Отсутствие наименьшей нижней границы;
7. Ничего из перечисленного.

Вопрос 3. Какие из перечисленных требований являются требованиями дискреционной политики?
1. все сущности идентифицированы;
2. задано множество ролей, каждой из которых ставится в соответствие некоторое множество прав доступа к сущностям;
3. каждый субъект обладает некоторым множеством ролей;
4. задана матрица доступов, каждая строка которой соответствует субъекту, а столбец – сущности КС, ячейка содержит список прав доступа субъекта к сущности;
5. задана решетка уровней конфиденциальности информации;
6. каждой сущности присвоен уровень конфиденциальности, задающий установленные ограничения на доступ к данной сущности;
7. каждому субъекту присвоен уровень доступа, задающий уровень полномочий данного субъекта в КС;
8. субъект обладает правом доступа к сущности КС тогда, когда он обладает ролью, которой соответствует множество прав доступа, содержащее право доступа к данной сущности.

Вопрос 4. Для каких систем ТМД существует алгоритм проверки безопасности?
1. для любых;
2. для ациклических;
3. для монооперационных;
4. для ациклических в канонической форме;
5. для любых в канонической форме;
6. ни для каких не существует.

Вопрос 5. Выберите из нижеприведенного списка расширения модели TakeGrant:
1. Де-факто-правила для поиска и анализа информационных потоков;
2. Де-юре-правила для поиска и анализа информационных потоков;
3. Алгоритм построения замыкания графов доступов и информационных потоков;
4. Алгоритм построения замыкания графа атак;
5. Способы анализа путей распространения прав доступа или информационных потоков;
6. Способы анализа путей распространения прав доступа и информационных потоков.

Вопрос 6. Какие из перечисленных требований являются требованиями мандатной политики?
1. все сущности идентифицированы;
2. задано множество ролей, каждой из которых ставится в соответствие некоторое множество прав доступа к сущностям;
3. каждый субъект обладает некоторым множеством ролей;
4. задана матрица доступов, каждая строка которой соответствует субъекту, а столбец – сущности КС, ячейка содержит список прав доступа субъекта к сущности;
5. задана решетка уровней конфиденциальности информации;

6. каждой сущности присвоен уровень конфиденциальности, задающий установленные ограничения на доступ к данной сущности;
7. каждому субъекту присвоен уровень доступа, задающий уровень полномочий данного субъекта в КС;
8. субъект обладает правом доступа к сущности КС тогда, когда он обладает ролью, которой соответствует множество прав доступа, содержащее право доступа к данной сущности.

Вопрос 7. Какие из перечисленных требований являются постулатами безопасности системы военных сообщений (СВС)?
1. в системе существует офицер безопасности;
2. системный офицер безопасности корректно разрешает доступ пользователей к сущностям и назначает уровни конфиденциальности устройств и множества ролей;
3. пользователь назначает или переназначает корректные уровни конфиденциальности сущностей, когда создает или редактирует в них информацию;
4. пользователь не может иметь более одной роли;
5. пользователь корректно направляет сообщения по адресатам и определяет множества доступа к созданным им самим сущностям;
6. пользователь правильно задает атрибут CCR контейнеров.

Открытые вопросы:

Вопрос 8. Опишите требования информационного невлияния, позволяющие в автоматной модели реализовать мандатную политику безопасности для решетки {Low, Middle, High};
Вопрос 9. Составьте команду системы ХРУ на передачу субъектом s субъекту s1 права удаления на принадлежащий s файл файл o;
Вопрос 10. Приведите алгоритм построения развернутого состояния АКФМТМД и алгоритм проверки безопасности систем АМТМД.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОК-7 - способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	Знать: основные модели доступа в информационной системе. Уметь: реализовывать основные модели доступа в информационной системе.	Практическая работа по подгруппам, собеседования, вопросы к зачету	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности

2.	ОПК-10 - способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Знать: методы формального описания модели злоумышленника. Уметь: формально описывать модель злоумышленника.	Практическая работа по подгруппам, собеседования, вопросы к зачету.	выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
3.	ОПК-2 - способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, тео	Знать: основные способы формального описания и анализа политик безопасности. Уметь: формально описывать и анализировать политику безопасности.	Практическая работа по подгруппам, собеседования, вопросы к зачету.	
4.	ОПК-4 - способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарным и и инновационными проектами	Знать: методы анализа модели угроз. Уметь: анализировать модель угроз.	Практическая работа по подгруппам, собеседования, вопросы к зачету.	
5.	ОПК-9 - способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знать: основные модели доступа в информационной системе. Уметь: реализовывать основные модели доступа в информационной системе.	Практическая работа по подгруппам, собеседования, вопросы к зачету.	
6.	ПК-1 - способность осуществлять подбор, изучение и обобщение научно-технической	Знать: методы формального описания модели злоумышленника.	Практическая работа по подгруппам, собеседования	

	информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	Уметь: формально описывать модель злоумышленника.	, вопросы к зачету.	
7.	ПК-2 - способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований	Знать: основные способы формального описания и анализа политик безопасности. Уметь: формально описывать и анализировать политику безопасности.	Практическая работа по подгруппам, собеседования, вопросы к зачету.	
8.	ПК-4 - способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знать: методы анализа модели угроз. Уметь: анализировать модель угроз.	Практическая работа по подгруппам, собеседования, вопросы к зачету.	

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. **Богульская, Н.А.** Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. — Красноярск : Сибирский федеральный университет, 2019. — 206 с. — ISBN 978-5-7638-4008-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/100055.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

7.2. Дополнительная литература:

1. **Воронцова, Е.А.** Программирование на C++ с погружением: практические задания и примеры кода - М.:НИЦ ИНФРА-М, 2016. – 80 с. – Режим доступа: http://znanium.com/bookread2.php?book=563294 (дата обращения 15.05.2020);
2. **Хорев, П.Б.** Объектно-ориентированное программирование с примерами на C#: Учебное пособие / Хорев П.Б. - М.: Форум, НИЦ ИНФРА-М, 2016. - 200 с. – Режим доступа: http://znanium.com/bookread2.php?book=529350 (дата обращения: 15.05.2020);
3. **Шаньгин, В.Ф.** Информационная безопасность компьютерных систем и сетей: Учебное пособие [Электронный ресурс] / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 416 с. – Режим доступа: http://znanium.com/bookread2.php?book=549989 (дата обращения 15.05.2020).

7.3. Интернет-ресурсы

- Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [On-line] (дата обращения: 15.05.2020).

7.4 Современные профессиональные базы данных и информационные справочные системы:

- Национальная электронная библиотека. - https://rusneb.ru/ [On-line] (дата обращения: 15.05.2020).

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Лицензионное ПО:**
  платформа для электронного обучения Microsoft Teams;
  MS Visual Studio;
  MS SQL Server.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

- лекционная аудитория с проектором;
- компьютерный класс.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020г.

ОПЕРАЦИОННЫЕ СИСТЕМЫ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Оленников Е.А. Операционные системы. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Операционные системы [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Оленников Е.А, 2020.

1. Пояснительная записка

Учебная дисциплина «Операционные системы» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Операционные системы» является дать целостное представление об архитектуре современных операционных систем.

Задачи дисциплины «Операционные системы»:

- познакомить с историей развития ОС;
- дать представление об основных функциях, принципах построения и видах ОС;
- дать представление о методах управления основными вычислительными ресурсами ЭВМ;
- дать представление об управлении устройствами вода-вывода;
- познакомить с общими подходами к реализации файловых систем и организацией популярных файловых систем;
- познакомить с архитектурой современных ОС.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Информатика».

Дисциплина «Операционные системы» способствует освоению следующих дисциплин: «Администрирование операционных систем», «Безопасность операционных систем».

1.2.Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОПК-7: способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения		знать: историю развития ОС; основные функции ОС, принципы построения ОС, основные архитектурные решения, применяемые при разработке ОС; основные подсистемы современных ОС и их назначение; уметь: применять полученные знания при администрировании и защите ОС; применять полученные знания к различным предметным областям; работать с технической литературой и специализированными информационными ресурсами;
ПК-2: способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке		знать: основные функции ОС, принципы построения ОС, основные архитектурные решения, применяемые при разработке ОС; основные подсистемы современных

защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований		ОС и их назначение; принципы управления основными вычислительными ресурсами ЭВМ; принципы управления процессами и потоками; технологии управления памятью; принципы организации ввода-вывода; структуру современных файловых систем и технологии распределения дискового пространства; принципы организации взаимодействия прикладного ПО с ОС и аппаратным обеспечением; архитектуру современных ОС; уметь: применять полученные знания при формировании комплекса мер по обеспечению информационной безопасности ОС; применять полученные знания к различным предметным областям; работать с технической литературой и специализированными информационными ресурсами;

* не предусмотрено

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		4 семестр
Общий объем зач. ед.	3	3
час.	108	108
Из них:		
Часы аудиторной работы (всего):	72	72
Лекции	36	36
Практические занятия		
Лабораторные/практические занятия по подгруппам	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	36	36
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет

3. Система оценивания

3.1. По данной дисциплине предусмотрен зачет. Оценка за зачет студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических работ, индивидуальных заданий. Эта оценка

характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины. Для получения зачета необходимо набрать не менее 61 балла.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «зачет» студент должен сдать минимум 75% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Введение в ОС. Архитектура, функции, принципы построения, классификация ОС.	10	4		2	0
2.	Управление процессами, алгоритмы планирования.	6	2		2	0
3.	Синхронизация процессов. Тупики.	16	4		8	0
4.	Управление памятью.	16	4		8	0
5.	Организация ввода - вывода в ОС.	6	2		2	0
6.	Файловая система. Общие положения.	8	4		0	0
7.	Обзор современных файловых систем.	16	6		4	0
8.	ОС семейства Windows NT. Общий обзор, архитектура.	10	4		2	0
9.	Unix-like системы. Общий обзор, архитектура.	20	6		8	0
	Итого (часов)	108	36		36	0

4.2. Содержание дисциплины (*модуля*) по темам

Введение в ОС. Архитектура, функции, принципы построения, классификация ОС. История развития ОС. Основные функции ОС. Основные принципы построения ОС. Ядро ОС. Архитектурные особенности современных ОС. Классификация ОС.

Практическая работа 1.

Предварительное знакомство с ОС Windows. Интерфейс пользователя (графический, командной строки). Интерфейс прикладного программирования.

Управление процессами, алгоритмы планирования. Понятие процесса. Информационные структуры процесса. Жизненный цикл процесса. Планирование процессов.

Практическая работа 2.

Создание процессов и потоков в ОС Windows. Получение системной информации о работающих процессах и потоках в ОС Windows.

Синхронизация процессов. Тупики. Критические ресурсы. Гонки. Критическая секция. Взаимное исключение с активным ожиданием. Аппаратная поддержка взаимоисключений. Семафоры. Мониторы. Понятие тупика. Невыгружаемые ресурсы. Условия возникновения тупиков. Методы борьбы с тупиками.

Практическая работа 3.

Синхронизация процессов. Использование алгоритмов синхронизации.

Практическая работа 4.

Синхронизация процессов. Использование объектов ожидания (события, мьютексы) и критических секций для синхронизации процессов в ОС Windows.

Практическая работа 5.

Синхронизация процессов. Использование объектов ожидания (семафоры) для синхронизации процессов в ОС Windows.

Практическая работа 6.

Моделирование тупиков. Реализация методов борьбы с тупиками.

Управление памятью. Основные функции ОС по управлению памятью. Типы адресов. Методы распределения памяти. Кэш-память. Алгоритмы замещения страниц. Политика распределения памяти. Регулирование загрузки. Политика очистки страниц.

Практическая работа 7.

Получение системной информации об использовании памяти в ОС Windows.

Практическая работа 8.

Использование виртуальной памяти в своих приложениях в ОС Windows.

Практическая работа 9.

Использование технологии File Mapping в ОС Windows.

Практическая работа 10.

Работа с кучами в ОС Windows.

Организация ввода -вывода в ОС. Устройства и программное обеспечение ввода-вывода. Реализации доступа к управляющим регистрам и буферам. Прямой доступ к памяти (DMA). Программные уровни и функции ввода-вывода.

Практическая работа 11.

Работа с портами ввода-вывода.

Файловая система. Общие положения. Понятие файла, каталога, файловой системы (ФС). Основные функции ФС. Иерархия каталогов. Логическая организация ФС. Операция над файлами и каталогами. Общая модель ФС. Структура ФС на диске. Методы выделения дискового пространства.

Обзор современных файловых систем. **Логическая организация FAT, NTFS, UFS, ExtFS.**

Практическая работа 12.

Изучение логической организации ФС FAT 12/32.

Практическая работа 13.

Изучение логической организации ФС NTFS.

ОС семейства Windows NT. Общий обзор, архитектура. Обзор архитектуры ОС семейства Windows NT.

Практическая работа 14.

Изучение устройства ОС Windows. Процесс загрузки. Основные приемы работы в командной строке. Работа с реестром ОС Windows.

ОС семейства Unix. Общий обзор, архитектура. Общий обзор, архитектура. Обзор архитектуры ОС семейства Unix.

Практическая работа 15.

Общее знакомство с Unix-like системами. Дистрибутивы Linux. Установка Unix-like системы.

Практическая работа 16.

Основные приемы работы в командной строке, разработка сценариев в Unix-like системах.

Практическая работа 17.

Интерфейс Posix. Разработка простой программы в Unix-like системе.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Введение в ОС. Архитектура, функции, принципы построения, классификация ОС.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
2.	Управление процессами, алгоритмы планирования.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
3.	Синхронизация процессов. Тупики.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
4.	Управление памятью.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
5.	Организация ввода -вывода в ОС.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
6.	Файловая система. Общие положения.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
7.	Обзор современных файловых систем	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
8.	ОС семейства Windows NT. Общий обзор, архитектура.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
9.	Unix-like системы. Общий обзор, архитектура.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение основной и дополнительной литературы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации – зачет. Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса.

Вопросы к зачету.

1. Понятие операционной системы. Операционная система как виртуальная машина. Операционная система как система управления ресурсами. Операционная система как постоянно функционирующее ядро.
2. Понятие операционной среды. Программная среда. Основная и дополнительная программная среда.
3. Эволюция ОС.
4. Основные функции операционных систем
5. Основные принципы построения ОС
6. Архитектура операционной системы. Общий подход. Привилегированный и пользовательский режимы работы.
7. Архитектурные особенности современных операционных систем. Монолитное ядро. Слоеные системы. Виртуальные машины. Микроядерная архитектура. Смешанные системы.
8. Классификация операционных систем. Особенности областей применения.
9. Классификация операционных систем. Поддержка многозадачности.
10. Классификация операционных систем. Вытесняющая и не вытесняющая многозадачность.
11. Классификация операционных систем. Поддержка многонитевости.
12. Классификация операционных систем по способу взаимодействия с компьютером.
13. Классификация операционных систем по типу централизации.
14. Классификация операционных систем. Многопроцессорная обработка.
15. Классификация операционных систем. Поддержка многопользовательского режима.
16. Классификация операционных систем по типу аппаратуры.
17. Классификация операционных систем. Особенности областей использования
18. Классификация операционных систем. Особенности методов построения.
19. Понятие процесса. Состояния процесса. Информационные структуры процесса.
20. Планирование процессов. Уровни планирования. Основные цели планирования.
21. Алгоритмы планирования процессов.
22. Вытесняющая и не вытесняющая многозадачность
23. Синхронизация процессов. Критические ресурсы. Гонки. Критические секции.
24. Программные алгоритмы организации взаимодействия процессов. Запрет прерываний. Блокирующие переменные.
25. Программные алгоритмы организации взаимодействия процессов. Семафоры. Монитор. Сообщения
26. Понятие тупика. Условия возникновения тупиков. Основные направления борьбы с тупиками.
27. Средства синхронизации потоков в ОС Windows. Функции и объекты ожидания.
28. Основные функции ОС по управлению памятью. Типы адресов.
29. Методы распределения памяти без использования дискового пространства. Распределение памяти фиксированными разделами. Распределение памяти разделами переменной величины. Распределение памяти перемещаемыми разделами
30. Понятие виртуальной памяти
31. Методы распределения памяти с использованием дискового пространства. Страничное распределение памяти

32. Сегментное распределение памяти
33. Странично-сегментное распределение памяти
34. Свопинг
35. Понятие файловой системы. Файл. Типы и атрибуты файлов. Логическая организация файла.
36. Операции над файлами и каталогами. Защита файлов.
37. Общая модель файловой системы.
38. Методы выделения дискового пространства.
39. Управление свободным и занятым дисковым пространством.
40. Файловая система FAT 12/16/32 – логическая и физическая организация.
41. Файловая система NTFS – логическая и физическая организация.
42. Файловая система UFS2– логическая и физическая организация.
43. Файловая система Ext2FS – логическая и физическая организация.
44. Реализации доступа к управляющим регистрам и буферам.
45. Прямой доступ к памяти (DMA).
46. Программные уровни и функции ввода-вывода.
47. Архитектурные особенности ОС Windows NT.
48. Архитектурные особенности ОС семейства Unix.
49. Архитектурные особенности ОС Linux.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОПК-7: способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	**Знает**: историю развития ОС; основные функции ОС, принципы построения ОС, основные архитектурные решения, применяемые при разработке ОС; основные подсистемы современных ОС и их назначение; **Умеет**: применять полученные знания при администрировании и защите ОС; применять полученные знания к различным предметным областям; работать с технической литературой и специализированными информационными ресурсами;	Практическая работа. Зачет.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации

				обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-2: способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований	**Знает**: основные функции ОС, принципы построения ОС, основные архитектурные решения, применяемые при разработке ОС; основные подсистемы современных ОС и их назначение; принципы управления основными вычислительными ресурсами ЭВМ; принципы управления процессами и потоками; технологии управления памятью; принципы организации ввода-вывода; структуру современных файловых систем и технологии распределения дискового пространства; принципы организации взаимодействия прикладного ПО с ОС и аппаратным обеспечением; архитектуру современных ОС; **Умеет**: применять полученные знания при формировании комплекса мер по обеспечению информационной безопасности ОС; применять полученные знания к различным предметным областям; работать с технической литературой и специализированными информационными ресурсами;	Практическая работа. Зачет.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Сафонов, В. О. Основы современных операционных систем : учебное пособие / В. О. Сафонов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 868 с. — ISBN 978-5-9963-0495-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100347 (дата обращения: 15.05.2020).

7.2. Дополнительная литература:

2. Котельников, Е. В. Введение во внутреннее устройство Windows : учебное пособие / Е. В. Котельников. — 2-е изд. — Москва : ИНТУИТ, 2016. — 260 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100722 (дата обращения: 15.05.2020).

7.3. Интернет-ресурсы

1. вузовские электронно-библиотечные системы учебной литературы.
2. доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru.
3. https://intuit.ru/
4. https://docs.microsoft.com/
5. https://www.linux.org/
6. http://www.unix.org/

7.4 Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) https://icdlib.nspu.ru/
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА https://rusneb.ru/
- Справочная правовая система КонсультантПлюс http://www.consultant.ru/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Программное обеспечение виртуализации: VMWare, VirtualBox или другое.
- Операционная система Windows 7 или более поздние версии.
- Операционная система Linux, Unix-like система.
- Средства разработки: Microsoft Visual Studio.
- Офисный пакет.
- Платформа для электронного обучения Microsoft Teams.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Лекционная аудитория с проектором. Компьютерный класс с установленным ПО.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Зулькарнеев И.Р. Организационное и правовое обеспечение информационной безопасности. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» опубликована на сайте ТюмГУ: Организационное и правовое обеспечение информационной безопасности [электронный ресурс] / Режим доступа: https://www.utmn.ru/sveden/education/#

© Тюменский государственный университет, 2020.
© Зулькарнеев И.Р., 2020.

1. Пояснительная записка

Целью преподавания дисциплины «Организационное и правовое обеспечение информационной безопасности» является раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, понятие и виды компьютерных преступлений, а также приобретение студентами знаний по организационному обеспечению защиты информации и формирование некоторых практических навыков работы.

Задачи дисциплины– дать основы:

- информационного законодательства Российской Федерации;
- правил лицензирования и сертификации в области защиты информации;
- международного законодательства в области защиты информации;
- знаний о компьютерных преступлениях;
- построения систем организационной защиты объектов информатизации

1.1. Место дисциплины (модуля) в структуре образовательной программы

Данная дисциплина входит в блок Б1, Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Основы информационной безопасности».

Дисциплина «Организационное и правовое обеспечение информационной безопасности» преподается в 10 семестре, обеспечиваемых дисциплин нет, вырабатываемые компетенции обеспечивают выполнение выпускной квалификационной работы.

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (модуля)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОПК-5: способностью использовать нормативные правовые акты в своей профессиональной деятельности		Знает: нормативные правовые акты Российской Федерации в области обработки и защиты информации, их содержание, предмет регулирования и сферу применения; основные понятия, термины и определения в области обработки и защиты информации; Умеет: применять нормативные правовые акты Российской Федерации в области обработки и защиты информации для конкретных задач и ситуаций в области защиты информации.
ОПК-9: способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных		Знает: основные угрозы безопасности информации; этапы создания системы защиты информации; виды защищаемой информации и информационных систем, требования по их защите; порядок проведения аттестации объекта информатизации; Умеет:

системах с учетом угроз безопасности информации		сформировать перечень требований по защите информационной системы;
ПК-6: способностью участвовать в разработке проектной и технической документации		Знает: правила разработки технического задания на создание АС в защищенном исполнении; правила разработки технического проекта на создание системы защиты информации; необходимые для написания документов НПА и ГОСТы; Умеет: разрабатывать проекты документов Техническое задание и Технический проект на создание системы защиты информации;
ПК-14: способностью организовать работы по выполнению режима защиты информации, в том числе ограниченного доступа		Знает: порядок внедрения режима коммерческой тайны; порядок отнесения сведений к гостайне; грифы секретности и уровни допуска к гостайне; Умеет: определять порядок и состав действий по внедрению коммерческой тайны;
ПК-16: разрабатывать проекты нормативных, правовых и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем		Знает: состав и принципы написания организационно-распорядительной документации по защите информации; способы использования и обозначения требований по защите информации в организационно-распорядительной документации; Умеет: разрабатывать проекты организационно-распорядительной документации по защите информации;

* не предусмотрено

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Часов в семестре**
			10 семестр
Общая трудоемкость	**зач. ед.**	5	5
	час	180	180
Из них:			
Часы аудиторной работы (всего):		72	72
Лекции		36	36
Практические занятия		36	36
Лабораторные / практические занятия по подгруппам		0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося		108	108

Вид промежуточной аттестации (экзамен)		Экзамен

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (135-балльной) и традиционной (5-балльной) систем оценок.

Экзаменационная оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических занятий, индивидуальных домашних заданий, контрольной работы, коллоквиумов и тестов. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

130 - 135 баллов – отлично;

115 - 129 баллов - хорошо;

Студент, у которого сумма набранных баллов, оказалась меньше 115, должен сдать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 теоретических вопроса. Для получения оценки «удовлетворительно» студентом должно быть сдано минимум 80% практических работ и сделан ответ на 2 вопроса из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы, и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен сдать минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен детально раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы, и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен сдать все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами.

Примечание. Студент, желающий исправить экзаменационную оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена.

Баллы проставляются за посещение лекционных и практических занятий и активную работу на них, а также за выполненные практические задания по каждой теме дисциплины, тестовые задания и коллоквиумы.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№	Наименование тем и/или разделов	Объем дисциплины (модуля), час				
		Всего	Виды аудиторной работы (в час)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные / практические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Законодательство РФ в сфере информационной безопасности	20	4	4	0	

2.	Практика правонарушений в области ИБ	20	4	4	0	
3.	Государственная система защиты информации РФ	10	2	2	0	
4.	Организация режима коммерческой тайны	30	6	6	0	
5.	Защита государственной тайны	20	4	4	0	
6.	Документация в области ИБ	20	4	4	0	
7.	Лицензируемая деятельность в области ИБ	20	4	4	0	
8.	Проектирование системы защиты информации	20	4	4	0	
9.	Аттестация объектов информатизации	20	4	4	0	
	Итого (часов)	180	36	36	0	2

4.2. Содержание дисциплины *(модуля)* по темам

Законодательство РФ в сфере информационной безопасности.

Основные нормативно-правовые акты РФ и ГОСТы в области защиты информации: содержание, предмет регулирования и сфера применения. Иерархия НПА.

Практическая работа 1.

НПА в области защиты информации.

Практика правонарушений в области ИБ.

Виды ответственности за правонарушения в области ИБ. Статья 272, статья 273 и статья 274 Уголовного кодекса РФ. Кодекс Российской Федерации об административных правонарушениях, в сфере информационной безопасности, составление протоколов об указанных административных правонарушениях

Практическая работа 2.

Правонарушения в области ИБ.

Государственная система защиты информации РФ.

Принципы правового регулирования в области защиты информации. Уровни власти и их участие в обеспечении информационной безопасности. Доктрина информационной безопасности РФ.

Практическая работа 3.

Примеры атак и утечек информации в РФ и за рубежом.

Организация режима коммерческой тайны.

Понятие коммерческой тайны. Основные этапы и мероприятия по внедрению режима коммерческой тайны.

Практическая работа 4.
Составление акта об инциденте информационной безопасности.

Защита государственной тайны
Понятие государственной тайны. Перечень сведений, относящихся к гостайне. Порядок отнесения сведений к гостайне. Грифы секретности. Уровни допуска к гостайне. Ограничения, накладываемые допуском к гостайне. Ответственность за разглашение гостайны.

Практическая работа 5.
Определение сведений, относящихся к гостайне.

Документация в области ИБ.
Понятие и назначение документации в области ИБ. Иерархия организационно-распорядительной документации в области ИБ. Их назначение, содержания, правила составления и внедрения.

Практическая работа 6.
Разработка инструкции/регламента по защите информации.

Лицензируемая деятельность в области ИБ.
Лицензирование ФСБ России и ФСТЭК России в области ИБ: регулирующие НПА, применение, условия получения.

Практическая работа 7.
Подготовка предприятия к получению лицензии ФСБ России или ФСТЭК России.

Проектирование системы защиты информации.
Этапы создания системы защиты информации. Государственные информационные системы. Определение и порядок защиты. Техническое задание и Технический проект на создание системы защиты информации: понятие, состав, назначение и правила оформления.

Практическая работа 8.
Разработка технического проекта на создание системы защиты информации.

Аттестация объектов информатизации.
Аттестация объекта информатизации на соответствие требованиям по защите информации. Необходимость применения, варианты проведения, этапы проведения, регламентирующие и результирующие документы. Виды защищаемых информационных систем, их категорирование и требования по защите.

Практическая работа 9.
План аттестационных испытания для определенного вида информационной системы.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ Темы	Темы	Формы СРС, включая требования к подготовке к занятиям

1.	Законодательство РФ в сфере информационной безопасности	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
2.	Практика правонарушений в области ИБ	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
3.	Государственная система защиты информации РФ	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
4.	Организация режима коммерческой тайны	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
5.	Защита государственной тайны	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
6.	Документация в области ИБ	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
7.	Лицензируемая деятельность в области ИБ	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
8.	Проектирование системы защиты информации	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
9.	Аттестация объектов информатизации	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение основной и дополнительной литературы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1 Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации – экзамен. Экзамен проходит в традиционной форме, по билетам. В билете – 2 теоретических вопроса.

Теоретические вопросы:

1. Основные нормативные правовые акты в области защиты информации, их предмет регулирования и сфера применения. (ФЗ, Постановления Правительства и Указы Президента)
2. Основные нормативные правовые акты (НПА ФСТЭК России, ФСБ России) и ГОСТы в области защиты информации, их предмет регулирования и сфера применения
3. Правовое положение обладателя информации (права, обязанности)
4. Деятельность в области защиты информации: содержание и требования.
5. Виды ответственности за правонарушения в области ИБ.
6. Понятие коммерческой тайны. Основные этапы и мероприятия по внедрению режима коммерческой тайны.
7. Этапы создания системы защиты информации.
8. Понятие и назначение документации в области ИБ.

9. Иерархия организационно-распорядительной документации в области ИБ. Их назначение, содержания, правила составления и внедрения.

10. Виды защищаемой информации и информационных систем (с примерами)

11. Лицензирование ФСБ России в области ИБ: регулирующие НПА, применение, условия получения.

12. Лицензия ФСТЭК России по ТЗКИ: Регулирующие НПА, Применение, условия получения.

13. Лицензия по разработке и производству СрЗИ: регулирующие НПА, применение, условия получения.

14. Аттестация объекта информатизации на соответствие требованиям по защите информации. Необходимость применения, варианты проведения, этапы проведения, регламентирующие и результирующие документы.

15. Принципы правового регулирования в области защиты информации. Уровни власти и их участие в обеспечении информационной безопасности.

16. Категории информации в зависимости от категорий доступа и порядка предоставления и распространения (с примерами)

17. Общедоступная информация. Право на доступ к информации. Ограничение доступа к ней

18. Государственные информационные системы. Определение и порядок защиты.

19. Понятие государственной тайны. Перечень сведений, относящихся к гостайне. Порядок отнесения сведений к гостайне. Грифы секретности

20. Уровни допуска к гостайне. Ограничения, накладываемые допуском к гостайне. Ответственность за разглашение гостайны.

21. Понятие технического задания и технического проекта, состав, назначение и правила оформления.

6.2 Критерии оценивания компетенций:

Таблица 4

Карта критериев оценивания компетенций

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОПК-5: способностью использовать нормативные правовые акты в своей профессиональной деятельности	Знает: нормативные правовые акты Российской Федерации в области обработки и защиты информации, их содержание, предмет регулирования и сферу применения; основные понятия, термины и определения в области обработки и защиты информации; Умеет: применять нормативные правовые акты Российской Федерации в области обработки и защиты информации для конкретных задач и ситуаций в области защиты информации.	Практическая работа. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29

				«Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ОПК-9: способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знает: основные угрозы безопасности информации; этапы создания системы защиты информации; виды защищаемой информации и информационных систем, требования по их защите; порядок проведения аттестации объекта информатизации; Умеет: сформировать перечень требований по защите информационной системы;	Практическая работа. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
3.	ПК-6: способностью участвовать в разработке проектной и технической документации	Знает: правила разработки технического задания на создание АС в защищенном исполнении; правила разработки технического проекта на создание системы защиты информации; необходимые для написания документов НПА и ГОСТы; Умеет: разрабатывать проекты документов Техническое	Практическая работа. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных

		задание и Технический проект на создание системы защиты информации;		заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
4.	ПК-14: способностью организовать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Знает: порядок внедрения режима коммерческой тайны; порядок отнесения сведений к гостайне; грифы секретности и уровни допуска к гостайне; Умеет: определять порядок и состав действий по внедрению коммерческой тайны;	Практическая работа. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
5.	ПК-16: разрабатывать проекты нормативных, правовых и методических материалов, регламентирующих	Знает: состав и принципы написания организационно-распорядительной документации по защите информации; способы использования и обозначения требований по	Практическая работа. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при

	работу по обеспечению информационной безопасности компьютерных систем	защите информации в организационно-распорядительной документации; Умеет: разрабатывать проекты организационно-распорядительной документации по защите информации;		глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература:

1. Козьминых, С. И. Организационно-правовое обеспечение информационной безопасности : учебное пособие / С. И. Козьминых. - Тбилиси : Справедливая Грузия, 2020. - 309 с. - ISBN 978-9941-9663-2-3. - Текст : электронный. - URL: https://znanium.com/catalog/document?pid=1359091 (дата обращения: 20.05.2020)

7.2 Дополнительная литература:

1. Галатенко, В. А. Стандарты информационной безопасности : учебное пособие / В. А. Галатенко. — 2-е изд. — Москва : ИНТУИТ, 2016. — 307 с. — ISBN 5-9556-0053-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100511 (дата обращения: 20.05.2020)
2. Гришина, Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - Москва : Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.; . - (Высшее образование: Бакалавриат). ISBN 978-5-00091-007-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/491597 (дата обращения: 20.05.2020).

7.3 Интернет-ресурсы:

1. https://fstec.ru/ru/
2. http://fsb.ru/

7.4 Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) https://icdlib.nspu.ru/
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА https://rusneb.ru/
- Справочная правовая система КонсультантПлюс http://www.consultant.ru/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю):

- проектор;
- установленное ПО: MS Office

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Аудитория с проектором; ПК с установленным ПО: MS Office.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Зулькарнеев И.Р. Основы информационной безопасности. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины «Основы информационной безопасности» опубликована на сайте ТюмГУ: Основы информационной безопасности [электронный ресурс] / Режим доступа: https://www.utmn.ru/sveden/education/#

© Тюменский государственный университет, 2020.
© Зулькарнеев И.Р., 2020.

1. Пояснительная записка

Учебная дисциплина «Основы информационной безопасности» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Основной целью дисциплины «Основы информационной безопасности» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой информации; обучение основам информационной безопасности, принципам и методам защиты информации в информационных системах.

Задачи дисциплины «Основы информационной безопасности»:

- изучение основных методов и принципов обеспечения конфиденциальности, целостности и доступности информации в информационных системах;
- изучение типовых угроз безопасности информации при её обработке в информационных системах;
- изучение основных принципов обеспечения информационной безопасности;
- изучение основ построения модели угроз и политики безопасности;
- изучение основных моделей доступа.

1.1. Место дисциплины (модуля) в структуре образовательной программы

Данная дисциплина входит в блок Б1, Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Информатика».

Дисциплина «Основы информационной безопасности» способствует освоению следующих дисциплин: «Безопасность персональных данных», «Организационное и правовое обеспечение информационной безопасности», «Анализ и управление рисками информационной безопасности».

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (модуля)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-5: способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики		Знает: основные понятия информационной безопасности; важность и необходимость информационной безопасности на человека, организации и государства; уровни обеспечения информационной безопасности РФ; ответственность за преступления в информационной сфере в соответствии с законодательством РФ; основные регуляторы в области информационной безопасности; Умеет: оценить возможные последствия противоправных действий в области информационных технологий;
ОПК-3: способностью понимать значение		Знает:

информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации		основные термины и определения в области теории информации, информационных технологий и защиты информации; основные угрозы информационной безопасности; основные методы обеспечения безопасности информационных систем; основные методы поиска информации из открытых источников; Умеет: классифицировать информационные системы; классифицировать угрозы безопасности информации;
ОПК-5: способностью использовать нормативные правовые акты в своей профессиональной деятельности		Знает: нормативные правовые акты Российской Федерации в области защиты информации, их содержание, предмет регулирования и сферу применения; основные понятия, термины и определения в области защиты информации; Умеет: применять нормативные правовые акты Российской Федерации в области защиты информации для конкретных задач и ситуаций;

* не предусмотрено

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Часов в семестре**
			6 семестр
Общая трудоемкость	**зач. ед.**	3	3
	час	108	108
Из них:			
Часы аудиторной работы (всего):		72	72
Лекции		36	36
Практические занятия		36	36
Лабораторные / практические занятия по подгруппам		0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося		36	36
Вид промежуточной аттестации (экзамен)			Зачет

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной).

В 6 семестре по данной дисциплине предусмотрен зачет. Оценка за зачет студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время лабораторных работ, индивидуальных заданий. Эта

оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины. Для получения зачета необходимо набрать не менее 61 балла. Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать зачет.

Примечание:

Баллы проставляются за посещение лекционных и практических занятий и активную работу на них, а также за выполненные практические задания по каждой теме дисциплины, тестовые задания и коллоквиумы.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№	Наименование тем и/или разделов	Объем дисциплины (модуля), час				
		Всего	Виды аудиторной работы (в час)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные / практические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Основные понятия теории информационной безопасности	12	4	4	0	
2.	Классификация угроз информационной безопасности	12	4	4	0	
3.	Основные механизмы обеспечения информационной безопасности	12	4	4	0	
4.	Теоретический подход к обеспечению информационной безопасности	12	4	4	0	
5.	Нормативно-правовой подход к обеспечению информационной безопасности	12	4	4	0	
6.	Практический (экспериментальный) подход к обеспечению информационной безопасности	12	4	4	0	
7.	Построение модели угроз	12	4	4		
8.	Определение и разработка политики безопасности	12	4	4		
9.	Аудит информационной безопасности	12	4	4	0	
	Итого (часов)	108	36	36	0	0

4.2. Содержание дисциплины *(модуля)* по темам

Основные понятия теории информационной безопасности.

Основные понятия и определения: уязвимость, угроза, атака, эксплойт. Свойства информации: конфиденциальность, целостность, доступность.

Практическая работа 1.
Работа с основными понятиями информационной безопасности.

Классификация угроз информационной безопасности.
Классификация угроз информационной безопасности информационных систем по ряду базовых признаков: по природе возникновения, по степени преднамеренности появления, по непосредственному источнику угроз, по положению источника угроз, по степени зависимости от активности информационной системы, по степени воздействия на информационную систему и т.д.

Практическая работа 2.
Классификация угроз информационной безопасности.

Основные механизмы обеспечения информационной безопасности.
Определение и методы реализации идентификации, аутентификации, авторизации и аудита. Обеспечение аутентификации с помощью «секрета» и криптографии. Авторизация на основе дискреционной, мандатной, ролевой и атрибутивной модели доступа.

Практическая работа 3.
Реализация основных механизмов обеспечения информационной безопасности.

Теоретический подход к обеспечению информационной безопасности.
Формальные методы доказательства информационной безопасности информационной системы (верифицированная защита). Формальное описание обобщённой и вероятностной моделей систем защиты распределённой информационной системы. Формальное описание модели безопасности распределённой информационной системы, построенной с использованием теории графов и теории автоматов.

Практическая работа 4.
Применение теоретических подходов к обеспечению информационной безопасности.

Нормативно-правовой подход к обеспечению информационной безопасности.
Объекты правового регулирования при создании и эксплуатации системы информационной безопасности. Использование существующих нормативных актов для создания системы информационной безопасности. Основные положения руководящих правовых документов. Основные положения критериев TCSEC («Оранжевая книга»). Основные положения Руководящих документов ФСТЭК в области защиты информации. Определение и классификация несанкционированного доступа.

Практическая работа 5.
Применение нормативно-правового подхода к обеспечению информационной безопасности.

Практический (экспериментальный) подход к обеспечению информационной безопасности.
Уровни доступа к хранимой, обрабатываемой, защищаемой в информационной системе информации. Основные методы реализации угроз информационной безопасности. Проведение тестов на проникновение, аспекты практической безопасности. Принципы обеспечения информационной безопасности: системности, комплексности, непрерывности

защиты, разумной достаточности, гибкости управления и применения, открытости алгоритмов и механизмов защиты, простоты применения защитных мер и средств.

Практическая работа 6.

Применение экспериментальный подхода к обеспечению информационной безопасности.

Построение модели угроз.

Определение актуальных угроз безопасности информационных систем. Сканирование системы для выявления текущих уязвимостей с учётом существующих структурных и функциональных связей в системе. Базы данных (словари) уязвимостей. Среда Metasploit Framework.

Практическая работа 7.

Построение модели угроз.

Определение и разработка политики безопасности.

Понятие политики безопасности, модели политики безопасности. Дискреционная политика безопасности. Мандатная политика безопасности. Мандатная политика целостности. Политика информационной безопасности как основа организационных мероприятий. Контроль и моделирование как основные формы организационных действий при проверке действенности системы информационной безопасности. Разграничение прав доступа как основополагающее требование организационных мероприятий и их практическая реализация на объекте защиты.

Практическая работа 8.

Разработка политики безопасности.

Аудит информационной безопасности.

Аудит системы информационной безопасности. Определение уровня защищённости информационной системы. Количественная и качественная оценки рисков. Аудит системы информационной безопасности на объекте как основание для подготовки организационных и правовых мероприятий. Его критерии, формы и методы.

Практическая работа 9.

Аудит информационной безопасности

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ Темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Основные понятия теории информационной безопасности	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
2.	Классификация угроз информационной безопасности	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

3.	Основные механизмы обеспечения информационной безопасности	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
4.	Теоретический подход к обеспечению информационной безопасности	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
5.	Нормативно-правовой подход к обеспечению информационной безопасности	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
6.	Практический (экспериментальный) подход к обеспечению информационной безопасности	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
7.	Построение модели угроз	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
8.	Определение и разработка политики безопасности	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
9.	Аудит информационной безопасности	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение основной и дополнительной литературы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1 Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации – зачет. Зачет проходит в традиционной форме, по билетам. В билете – 2 теоретических вопроса.

Теоретические вопросы:

1) Определение информационной безопасности (ИБ). Определение конфиденциальности, целостности и доступности. Основные подходы к обеспечению ИБ.

2) Определение «уязвимости», «угрозы», «атаки» и «эксплойта». Модели угроз и виды угроз (антропогенные, техногенные, стихийные источники угроз).

3) Модель нарушителя: определение хакерства. Цели и задачи хакера. «Белые», «серые» и «чёрные» хакеры. Социальная инженерия: определение, задачи, примеры применения для нарушения конфиденциальности, целостности и доступности информации.

4) Основные механизмы обеспечения ИБ: идентификация, аутентификация, авторизация, аудит.

5) Парольные системы аутентификации. Стойкость парольных систем аутентификации. Взаимная проверка подлинности пользователей информационной системы.

6) Биометрические системы аутентификации. Основные методы взлома биометрических систем аутентификации.

7) Основные модели разграничения прав доступа: дискреционная, мандатная и ролевая модели доступа.

8) Криптографическая защита информации: определение шифрования, расшифрования, дешифрования, криптографического ключа, хеширования информации.

9) Симметричное и асимметричное шифрование. Примеры симметричного и асимметричного шифрования: шифр Виженера, алгоритм RSA.

10) Электронно-цифровая подпись (ЭЦП): определение ЭЦП, схема ЭЦП, определение сертификата открытого ключа, удостоверяющего центра. Инфраструктура открытых ключей (PKI).

11) Кодирование информации как средство обеспечения целостности информации. Примеры алгоритмов кодирования.

12) Стеганография как один из способов обеспечения конфиденциальности и целостности информации.

13) Формальные модели безопасности информационных систем (ИС): обобщенные модели систем защиты ИС; вероятностные модели систем защиты информации ИС; модели безопасности ИС, построенные с использованием теории графов; модели безопасности ИС, построенные с использованием теории автоматов.

14) Эталонные модели взаимодействия открытых ИС: TCP/IP и OSI. Структура моделей. Уязвимости канального уровня.

15) Эталонные модели взаимодействия открытых ИС: TCP/IP и OSI. Структура моделей. Уязвимости сетевого уровня.

16) Эталонные модели взаимодействия открытых ИС: TCP/IP и OSI. Структура моделей. Уязвимости транспортного уровня.

17) Эталонные модели взаимодействия открытых ИС: TCP/IP и OSI. Структура моделей. Уязвимости прикладного уровня.

18) Нормативный подход в обеспечении ИБ. Политика безопасности (ПБ), модель ПБ. Оранжевая книга, классы безопасности ИС.

19) Аспекты защиты интеллектуальной собственности. Проблемы «пиратства». Реверсивный инжиниринг (обратное проектирование): цели, задачи, основные методы.

20) Алгоритм оценки и анализа рисков безопасности ИС. Управление рисками безопасности ИС.

21) Технические каналы утечки информации: акустический и виброакустический каналы; оптический канал утечки; электромагнитный канал утечки информации, ПЭМИН; материальный канал утечки информации. Основные способы защиты от утечки.

22) Организационные, технические и режимные меры обеспечения информационной безопасности информационных систем.

23) Определение «вируса». Структура «вируса». Принцип работы антивирусных программ. Обфускация (запутывание программного кода) и деобфускация.

24) Атака типа «отказ в обслуживании»: DoS, DDoS. Принцип построения «зомби»-сетей, основные цели атаки. Доступность как одно из ключевых свойств информации.

6.2 Критерии оценивания компетенций:

Таблица 4

Карта критериев оценивания компетенций

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОК-5: способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной	Знает: основные понятия информационной безопасности; важность и необходимость информационной безопасности на человека, организации и государства; уровни обеспечения информационной безопасности РФ;	Практическая работа. Зачет.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и

	деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	ответственность за преступления в информационной сфере в соответствии с законодательством РФ; основные регуляторы в области информационной безопасности; Умеет: оценить возможные последствия противоправных действий в области информационных технологий;		правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ОПК-3: способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации	Знает: основные термины и определения в области теории информации, информационных технологий и защиты информации; основные угрозы информационной безопасности; основные методы обеспечения безопасности информационных систем; основные методы поиска информации из открытых источников; Умеет: классифицировать информационные системы; классифицировать угрозы безопасности информации;	Практическая работа. Зачет.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
3.	ОПК-5: способностью использовать нормативные правовые акты в	Знает: нормативные правовые акты Российской Федерации в области защиты информации, их содержание, предмет	Практическая работа. Зачет.	Компетенция сформирована при правильности и полноте ответов

	своей профессиональной деятельности	регулирования и сферу применения; основные понятия, термины и определения в области защиты информации; Умеет: применять нормативные правовые акты Российской Федерации в области защиты информации для конкретных задач и ситуаций;		на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература:

1. Кияев, В. И. Безопасность информационных систем : учебное пособие / В. И. Кияев, О. Н. Граничин. — 2-е изд. — Москва : ИНТУИТ, 2016. — 191 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100580 (дата обращения: 20.05.2020). - Режим доступа: для авторизир. пользователей.

7.2 Дополнительная литература:

1. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е. В. Глинская, Н. В. Чичварин. - Москва : ИНФРА-М, 2021. - 118 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016536-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/1178153 (дата обращения: 20.05.2020). - Режим доступа: по подписке.
2. Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1. - Текст: электронный. - URL: https://znanium.com/catalog/product/997105 (дата обращения: 20.05.2020). - Режим доступа: по подписке.

7.2 Дополнительная литература:

3. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е. В. Глинская, Н. В. Чичварин. - Москва : ИНФРА-М, 2021. - 118 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016536-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/1178153 (дата обращения: 20.05.2020)

4. Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1. - Текст: электронный. - URL: https://znanium.com/catalog/product/997105 (дата обращения: 20.05.2020)

7.3 Интернет-ресурсы:

1. http://fsb.ru/
2. http://fstec.ru/
3. http://www.consultant.ru/

7.4 Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) https://icdlib.nspu.ru/
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА https://rusneb.ru/
- Справочная правовая система КонсультантПлюс http://www.consultant.ru/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю):

- проектор;
- установленное ПО: MS Office

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Аудитория с проектором; ПК с установленным ПО: MS Office.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

РАЗРАБОТКА И ЗАЩИТА WEB-ПРИЛОЖЕНИЙ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Оленников А.А. Разработка и защита web-приложений. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Разработка и защита web-приложений [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Оленников А.А., 2020.

1. Пояснительная записка

Учебная дисциплина «Разработка и защита web-приложений» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Целью дисциплины «Разработка и защита web-приложений» является обучение студентов основам создания веб приложений, ознакомиться с современным серверным и сетевым оборудованием, изучить методики и способы защиты веб приложений и сетевого оборудования.

Задачи дисциплины «Разработка и защита web-приложений»:

- изучить устройство сети Интернет;
- изучить языки разметки документов;
- изучить протоколы http, https, ftp;
- изучить принцип работы веб сервера;
- принципы функционирования веб приложений;
- изучить средства разработки веб приложений;
- изучить наиболее распространённые веб серверы, их возможности и функционал;
- научиться создавать простейшие веб страниц;
- научиться использовать основные и дополнительные метатеги;
- изучить способы создания и настройки дополнительных инструментариев, позволяющие увеличивать посещаемость сайтов;
- изучить методы проверки и тестирования законченных сайтов;
- изучить подходы к проектированию веб сервера и локально-вычислительной сети с сетевым оборудованием;
- научиться организовывать способы защиты от различного рода сетевых атак на Web и DNS серверы, и сетевое оборудование;
- рассмотреть наиболее распространенные типы уязвимостей на сетевое оборудование;
- научиться настраивать веб сервер и его сетевые карты, роли DNS, IIS и другие для корректной работы сайта;
- научиться настраивать межсетевые экраны, коммутаторы, балансировку нагрузки;
- научиться организовывать серверные кластеры;
- научиться производить анализ защищенности веб приложения;
- научиться организовывать защиту веб приложений.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в базовую часть цикла естественно - научных дисциплин, блок Б1. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Языки программирования», «Системы управления базами данных», «Операционные системы», «Сети и системы передачи информации».

Дисциплина «Разработка и защита web-приложений» способствует освоению дисциплины: «Безопасность интернета вещей», «Защита программ и данных», «Управление IT проектами».

1.2.**Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)**

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)

ОПК-8 – способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач.	----------	**Знать:** устройство сети Интернет; языки разметки документов; протоколы http, https, ftp; принцип работы веб сервера; принципы функционирования веб приложений; средства разработки веб приложений; наиболее распространённые веб серверы, их возможности и функционал; способы создания простейших веб страниц; основные и дополнительные метатеги; способы создания и настройки дополнительных инструментариев, позволяющие увеличивать посещаемость сайтов; методы проверки и тестирования законченных сайтов; подходы к проектированию веб сервера и локально-вычислительной сети с сетевым оборудованием; способы защиты от различного рода сетевых атак на Web и DNS серверы, и сетевое оборудование; наиболее распространенные типы уязвимостей. **Уметь:** использовать средства разработки веб приложений; разрабатывать простые веб страницы на языке html; использовать основные и дополнительные метатеги; использовать дополнительный инструментарий, позволяющий увеличивать число посетителей и продвигать сайт в поисковых системах; настраивать веб сервер и его сетевые карты, роли DNS, IIS и другие для корректной работы сайта; настраивать межсетевые экраны, коммутаторы, балансировку нагрузки; организовывать серверные кластеры; производить анализ защищенности веб приложения; производить защиту веб приложения; производить устранение основных типов угроз.

* не предусмотрено

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы		**Всего часов**	**Часов в семестре**	
			5	6
Общая трудоемкость	**зач. ед.**	7	3	4
	час	252	108	144
Из них:				
Часы аудиторной работы (всего):		144	72	72
Лекции		72	36	36
Практические занятия		0	0	0
Лабораторные / практические занятия по подгруппам		72	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося		108	36	72
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Зачет	Экзамен

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной) и традиционной (5-балльной) систем оценок.

Количество баллов, необходимые для получения зачета в 5 семестре является интегрированной оценкой выполнения студентом заданий во время практических работ, индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины.

Для получения зачета необходимо набрать не менее 75 баллов.

Студент, у которого сумма набранных баллов, оказалась меньше 75, должен обязательно выполнить и сдать все практические работы и индивидуальные задания, а также подготовить ответы на вопросы, предложенные преподавателем.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «зачтено» студентом должны быть сданы все практические работы и индивидуальные задания, выдаваемые преподавателем в ходе семестра. В зависимости от качества выполненного задания за каждую работу может назначаться разное количество баллов. Изначально предусмотрено, если студент в ходе обучения выполняет в срок практические и индивидуальные задания, посещает лекции и активно работает на них – он автоматически набирает необходимое количество баллов для получения зачета.

Если студент выполняет практические и индивидуальные задания в срок, посещает лекции и активно работает на них, но качество практических работ и индивидуальных заданий неудовлетворительное – обучающийся имеет право доработать практические работы или индивидуальные задания, либо подготовить ответы на вопросы преподавателя.

В 6 семестре предусмотрен экзамен. Экзаменационная оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических работ, индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен. Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должно быть выполнено минимум 50% практических работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий

тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 75% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить экзаменационную оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
5 семестр						
1.	Введение. Устройство сети Интернет. Обзор современных веб технологий.	4	2	0	2	0
2.	DNS сервер и его роль в организации работы сайта.	8	4	0	4	0
3.	DNS записи, маршрутизация и обзор современных DNS серверов.	10	4	0	4	0
4.	Языки разметки документов. Гипертекстовая разметка XML.	6	2	0	0	0
5.	Средства разработки веб приложений. CMS – Системы управления контентом веб-сайтов.	8	4	0	2	0

6.	Протокол HTTP, веб сервер и веб клиент, прокси сервер.	8	4	0	2	0
7.	Создание простой web-страницы. Форматирование.	8	2	0	2	0
8.	Каскадные таблицы стилей (CSS).	8	2	0	4	0
9.	Метатеги основные и дополнительные.	8	2	0	4	0
10.	Системы индексации сайтов. Файл robots.txt и sitemap.xml.	10	2	0	4	0
11.	Веб-аналитика. Счетчики.	14	4	0	4	0
12.	JavaScript для WEB.	16	4	0	4	0
	Итого (часов) 5 семестр	108	36	0	36	0
6 семестр						
13	Защищенное делегирование с DNSSEC.	16	2	0	4	0
14	Межсетевые экраны. Настройка межсетевого экрана модели DFL-860e.	28	10	0	6	0
15	Способы реализации процесса балансировки нагрузки.	26	8	0	6	0
16	Веб сервер и DNS сервер. Виртуализация серверов и ролей.	24	6	0	8	0
17	Почтовый сервер. Принцип работы, настройка и администрирование.	18	4	0	6	0
18	Способы защиты от спама.	16	2	0	2	0
19	Организация антивирусной защиты на серверах и шлюзах.	16	4	0	4	0
	Итого (часов) 6 семестр	144	36	0	36	2

4.2. Содержание дисциплины (*модуля*) по темам

5 семестр

Тема 1. Введение. Устройство сети Интернет. Обзор современных веб технологий.

Практическая работа 1.

Работа с сервисом Whois. По доменному имени определить: 1. IP адрес сервера; 2. Назначение сайта; 3. Принадлежность к организации; 4. Месторасположение сервера (Страна, город).

Тема 2. DNS сервер и его роль в организации работы сайта.

Практическая работа 2.

Работа с корневыми DNS серверами 1. Разделиться группой на 3-и звена. 2. Определить общее количество главных корневых DNS серверов, выявить имя хостов и проверить актуальность IP адресов (протоколы IPv4 и IPv6); 3. Определить физическое

местоположение (страна, город, организация) DNS серверов; 4. Определить реплицирующие DNS серверы корневых зон по звеньям. 5. Для реплицирующих DNS серверов определить данные изложенные в пунктах 2 и 3.

Практическая работа 3.

DNS записи 1. Изучить и отразить в отчете все типы записей роли DNS для сетевых ОС Windows. 2. Какие типы записей необходимо прописать в роли DNS для корректной работы web-сайта, расположенном на этом же сервере. 3. В каких случаях применяют запись типа TXT? Привести примеры записи TXT. 4. Какой исчерпывающий набор записей необходим для корректной работы почтового сервера?

Тема 3. DNS записи, маршрутизация и обзор современных DNS серверов.

Практическая работа 4.

Сопоставление IP адресов с доменным именем. 1. Используя утилиту nslookup или другой инструмент, выполнить проверку доменов второго уровня на сопряжение с ip адресами. 2. Определить сколько и каких ip адресов закреплено за каждым доменным именем. 3. Должно быть рассмотрено не менее 20-ти доменов. 4. Выполните проверку DNS серверов (можно использовать данные из пункта 3) на возврат записей по запросу. Пример: В командной строке вводим Nslookup Default Server: ns.masterhost.ru Address: xxx.xxx.x.x:53 > set querytype=any > xxxxx.ru 5. Проверьте каждый DNS сервер в рамках рассматриваемого домена на предмет возврата записей. Пример: В командной строке продолжаем вводить, например: > server ns2.xxxx.ru Default Server: ns2.xxxx.ru Address: xx.xx.xxx.x > ls -d xxxx.ru 6. На основании полученных записей можно судить о настройках безопасности серверов. 7. Составить отчет о проделанной работе, в который должны войти все проанализированные записи с выделением критичных (то что не должно быть доступно пользователям из глобальной сети).

Практическая работа 5.

Настройка роли DNS Цель: Настроить сервер, предназначенный для публикации сайтов, приема и пересылки запросов DNS. Для этого: 1. Используя любую редакцию ОС MS Windows Server, выполнить настройки сетевого адаптера и присвоить ему статический IP-адрес. 2. Установить роль DNS. 3. Создать одну зону прямого просмотра (имя зоны назначаете самостоятельно). 4. Внести соответствующие записи необходимых типов в базу DNS. 5. Настроить зону обратного просмотра. 6. Организовать передачу зоны на другой доверенный сервер.

Тема 4. Языки разметки документов. Гипертекстовая разметка XML.

Тема 5. Средства разработки веб приложений. CMS – Системы управления контентом веб-сайтов.

Практическая работа 6.

Изучения средств разработки веб-приложений и их функционала.

Создание простой web-страницы. Создать Web-страницу (ознакомление с основными тэгами HTML). Добавьте в документ Test.htm тэги, с помощью которых можно задать цвет фона и шрифта, различное начертание шрифта, выравнивание (после внесения изменений, в документе выполнять команду Файл – Сохранить).

Тема 6. Протокол HTTP, веб сервер и веб клиент, прокси сервер.

Практическая работа 7.

Разработать структуру будущего сайта, посвященному любой тематике на выбор обучающегося.

Тема 7. Создание простой web-страницы. Форматирование.

Практическая работа 8.

Создание простой web-страницы. Задание №1. Добавьте в документ Test.htm тэги, с помощью которых можно вставить графическое изображение и гиперссылку на другую Web-страницу.

Задание №2. Добавьте в документ Test.htm атрибуты тэгов, с помощью которых можно отформатировать графическое изображение; в файле автобиография.htm сделайте картинку фоном документа, вставьте в него таблицу.
Задание №3.
Задание 3. Разработать главную и вспомогательные страницы будущего сайта с использованием необходимого инструментария.
Тема 8. Каскадные таблицы стилей (CSS).
Практическая работа 9.
Работа со стилями. 1. Создать простой сайт, состоящий из 5-ти страниц, наполненных текстовым и графическим контентом. 2. Связать все страницы с единым файлом CSS (лежащем в корне сайта) отвечающий за стили. 3. Обязательно применить любые стили к текстовому и графическому контенту на свое усмотрение. 4. При изменении параметров в файле CSS стили должны применяться ко всему сайту.
Практическая работа 10.
Применить и настроить стили CSS для разрабатываемого сайта.
Тема 9. Метатеги основные и дополнительные.
Практическая работа 11.
Применить необходимые метатеги для разрабатываемого сайта.
Тема 10. Системы индексации сайтов. Файл robots.txt и sitemap.xml.
Практическая работа 12.
Работа с файлами Robots.txt и Sitemap.xml. 1. Используя информация лекционного материала, создать файл Robots.txt и внести в него необходимые записи, разрешающие или запрещающие действия. 2. Используя портал https://www.mysitemapgenerator.com создать для любых действующих сайтов в зоне ME файлы Sitemap.xml. 3. Сравнить созданные файлы Sitemap.xml с существующими файлами, присутствующими в корне сайтов. 4. Показать любым доступным способом отличия между этими файлами. 5. Рассмотреть индивидуально каждому не менее 50 сайтов. 6. Отчет должен быть представлен в виде 50 папок (каждый сайт – имя папки). 7. В каждой папке должно находиться три файла: 1-созданный Sitemap.xml; 2-существующий Sitemap.xml, полученный с корня сайта; 3-текстовый файл с отличиями.
Тема 11. Веб-аналитика. Счетчики.
Практическая работа 13.
Выполнить информационный поиск и выявить порталы, которые используют счетчики и системы формирования статистики.
Практическая работа 14.
Настроить счетчики и системы статистики для разрабатываемого сайта.
Тема 12. JavaScript для WEB.
Практическая работа 15.
Используя технологию JavaScript, разработать окно авторизации для разрабатываемого сайта.
Практическая работа 16.
Используя технологию JavaScript, предусмотреть и проработать динамические элементы для разрабатываемого сайта.

6 семестр
Тема 13. Защищенное делегирование с DNSSEC.
Практическая работа 1.

Серверы работающие с использованием расширения DNSSEC. Используя современные инструменты, попытайтесь выявить не менее 20 DNS серверов, на которых зоны подписаны DNSsec. Обязательно в отчете указать сведения подтверждающие эту информацию, а именно отразить DNSKEY и записи DS.

Практическая работа 2.
Подпись зоны DNSSEC. 1. Используя любую редакцию ОС MS Windows Server, выполнить настройки сетевого адаптера и присвоить ему статический IP-адрес. 2. Установить роль DNS. 3. Создать домен второго урвня на DNS сервере в зоне прямого просмотра. В настройки DNS сервера внести записи типа A для корректного ответа вэб-клиентам при обращении к вэб-серверу. 4. Подписать данную зону расширением DNSSEC.
Тема 14. Межсетевые экраны. Настройка межсетевого экрана модели DFL-860e.
Практическая работа 3.
Публикация сайта на платформе IIS.
Публикация сайта на локальной машине 1. Используя любую редакцию ОС MS Windows Server, необходимо на виртуальной машине опубликовать разработанный ранее сайт. 2. Для этого необходимо установить роли DNS и IIS в среде Windows и выполнить необходимые настройки. 3. Создать домен второго и третьего уровней (имя домена назначаем самостоятельно). 4. Предусмотреть ответ сайта только по протоколу http, по двум доменам. 5. Работу желательно выполнять вдвоем. 6. После выполнения всех настроек, данную работу нужно продемонстрировать. Для этого один компьютер выступает в роли сервера, второй – в роли клиента. Соединение организовать физическое по проводной или беспроводной связи.
Практическая работа 4.
Публикация сайта на физическом сервере. На предоставленном физическом сервере с операционной системой Microsoft Windows Server и установленными ролями DNS и IIS настроить публикацию сайта таким образом, чтобы по первому сетевому интерфейсу отвечал только сайт с доменом второго уровня, а по второму сетевому интерфейсу – сайт с доменом третьего уровня. Физически сайт должен находится на разделе жесткого диска, выделенный под файловый ресурс.
Практическая работа 5.
Проверка сервера на уязвимость. Используя наработки практической работы №4 и современные инструменты, выполнить анализ сервера на предмет уязвимости и подготовить соответствующий отчет, представляющий исчерпывающую информацию о степени защищенности сервера, а также предложить рекомендации по защите сервера.
Практическая работа 6.
Изучение межсетевого экрана DFL-860e и его первоначальная настройка.
Выполнить необходимые начальные настройки межсетевого экрана. Настроить системное времея и его синхронизацию. Настроить адресную книгу и сервисы по предложенным условиям преподавателя. Выполнить настройки таймаутов.
Практическая работа 7.
Работа с межсетевым экраном DFL-860e.
Выполнить необходимые начальные настройки межсетевого экрана и организовать доступ к серверу через межсетевой экран по протоколам http и ftp. Настроить адресную книгу, сетевые правила и необходимые сервисы для корректной работы с ресурсами. Схема сети 1. Сервер подключается к порту Wan1, а все пользователи к портам Lan. Схема сети 2. Сервер подключается к порту любому порту Lan, а все пользователи к портам Wan через коммутатор. В обоих случаях нужно придерживаться максимальной защищенности, как со стороны сервера, так и со стороны клиента.
Практическая работа 8.
Анализ сетевой инфраструктуры. Используя результаты практической работы 7 и современные инструменты, выполнить анализ сервера и межсетевого экрана на предмет уязвимости и подготовить соответствующий отчет, представляющий исчерпывающую информацию о степени защищенности сервера, а также предложить рекомендации по защите сервера.
Тема 15. Способы реализации процесса балансировки нагрузки.
Практическая работа 9.

Виды и способы организации балансировки нагрузки. Изучить виды и способы организации балансировки нагрузки. Рассмотреть программные и аппаратные решения балансировки нагрузки. Составить отчет о проделанной работе.

Тема 16. Веб сервер и DNS сервер. Виртуализация серверов и ролей.

Практическая работа 10.

Организация балансировки нагрузки. На предоставленном физическом сервере с двумя виртуальными машинами на операционной системой Microsoft Windows Server и установленными ролями DNS и IIS, настроить публикацию сайта. Первая виртуальная машина должна прослушивать первый сетевой интерфейс; вторая виртуальная машина должна прослушивать второй сетевой интерфейс. Организовать балансировку нагрузки между сетевыми интерфейсами и соответственно виртуальными машинами. Организацию балансировки предусмотреть как аппаратную, так и программную. Процесс работы продемонстрировать.

Тема 17. Почтовый сервер. Принцип работы, настройка и администрирование.

Практическая работа 11.

Настройка почтового сервера. На предоставленном физическом сервере, установить роль почтового сервера, выполнить необходимые настройки для работы в сети и создать почтовый домен.

Тема 18. Способы защиты от спама.

Практическая работа 12.

Способ фильтрации спама на DFL-860e. Используя результаты практической работы 11 и межсетевой экран DFL-860e, выполнить настройки, отвечающие за фильтрацию спама.

Тема 19. Организация антивирусной защиты на серверах и шлюзах.

Практическая работа 13.

Работа с антивирусом. На предоставленном физическом сервере установить антивирус Касперского (редакция Kaspersky Endpoint Security). Выполнить настройки антивируса, его политик, задач и других параметров).

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
5 семестр		
1.	Введение. Устройство сети Интернет. Обзор современных веб технологий.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
2.	DNS сервер и его роль в организации работы сайта.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
3.	DNS записи, маршрутизация и обзор современных DNS серверов.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
4.	Языки разметки документов. Гипертекстовая разметка XML.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
5.	Средства разработки веб приложений. CMS –	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.

	Системы управления контентом веб-сайтов.	
6.	Протокол HTTP, веб сервер и веб клиент, прокси сервер.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
7.	Создание простой web-страницы. Форматирование.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
8.	Каскадные таблицы стилей (CSS).	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
9.	Метатеги основные и дополнительные.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
10.	Системы индексации сайтов. Файл robots.txt и sitemap.xml.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
11.	Веб-аналитика. Счетчики.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
12.	JavaScript для WEB.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
6 семестр		
13.	Защищенное делегирование с DNSSEC.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
14.	Межсетевые экраны. Настройка межсетевого экрана модели DFL-860e.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
15.	Способы реализации процесса балансировки нагрузки.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
16.	Веб сервер и DNS сервер. Виртуализация серверов и ролей.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
17.	Почтовый сервер. Принцип работы, настройка и администрирование.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
18.	Способы защиты от спама.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
19.	Организация антивирусной защиты на серверах и шлюзах.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение рекомендованной основной и дополнительной литературы.
3. Выполнение практической работы.
4. Защита практической работы с объяснениями.

Контроль за самостоятельной работой осуществляется при выполнении обучающимся практической работы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации в 5 семестре – зачет. Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса.

Форма проведения промежуточной аттестации в 6 семестре – экзамен. Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса.

Вопросы к зачету (5 семестр).

1. Устройство сети Интернет, виды и классы сетей.
2. DNS сервер и его роль в сети Интернет и сети организации.
3. Виды записей роли DNS и их назначение.
4. DNS сервер и его роль в работе сайта.
5. Языки разметки документов. Гипертекстовая разметка XML.
6. Средства разработки веб приложений. Основные отличия.
7. CMS – Системы управления контентом веб-сайтов и их функционал.
8. Виды протоколов для работы в веб среде, их назначение.
9. Протокол HTTP и FTP.
10. Механизм работы клиент-серверной технологии.
11. Веб сервер и роли поддерживающие работу веб приложений.
12. Прокси сервер, его роль и механизма работы.
13. Создание простой web-страницы. Форматирование.
14. Каскадные таблицы стилей (CSS).
15. Основные и дополнительные метатеги.
16. Системы индексации сайтов.
17. Файл robots.txt и sitemap.xml.
18. Веб аналитика, сбор, настойка, формирование.
19. Счетчики сайтов и системы кэширования.
20. Коды ошибок веб серверов, их отличие и назначение.
21. JavaScript разработки применяемые для веб сайтов.
22. Пошаговая настройка сервера для публикации сайта.
23. Способы исключения сайта из индекса поисковых систем.
24. Виды веб серверов, их отличие и функционал.
25. Код html, роль заголовков типа «H» и метатегов.
26. Способы ускорения отображения веб страниц на стороне клиента.
27. Подключение сторонних сервисов для веб сайтов.
28. Назначение файлов Robots.txt и Sitemap.xml.
29. Назначение регистратора и корневых DNS серверов.
30. Тестирование DNS серверов со стороны регистратора, и ошибки в настройках.

Вопросы к экзамену (6 семестр).

1. Устройство сети Интернет, виды и классы сетей.
2. DNS сервер и его роль в сети Интернет и сети организации.
3. Виды записей роли DNS и их назначение.
4. DNS сервер и его роль в работе сайта.
5. Языки разметки документов. Гипертекстовая разметка XML.
6. Средства разработки веб приложений. Основные отличия.

7. CMS – Системы управления контентом веб-сайтов и их функционал.
8. Виды протоколов для работы в веб среде, их назначение.
9. Протокол HTTP и FTP.
10. Механизм работы клиент-серверной технологии.
11. Веб сервер и роли поддерживающие работу веб приложений.
12. Прокси сервер, его роль и механизма работы.
13. Создание простой web-страницы. Форматирование.
14. Каскадные таблицы стилей (CSS).
15. Основные и дополнительные метатеги.
16. Системы индексации сайтов.
17. Файл robots.txt и sitemap.xml.
18. Веб аналитика, сбор, настойка, формирование.
19. Счетчики сайтов и системы кэширования.
20. Коды ошибок веб серверов, их отличие и назначение.
21. JavaScript разработки применяемые для веб сайтов.
22. Пошаговая настройка сервера для публикации сайта.
23. Способы исключения сайта из индекса поисковых систем.
24. Виды веб серверов, их отличие и функционал.
25. Код html, роль заголовков типа «H» и метатегов.
26. Способы ускорения отображения веб страниц на стороне клиента.
27. Подключение сторонних сервисов для веб сайтов.
28. Назначение файлов Robots.txt и Sitemap.xml.
29. Назначение регистратора и корневых DNS серверов.
30. Тестирование DNS серверов со стороны регистратора, и ошибки в настройках.
31. Назначение расширения DNSSEC.
32. Межсетевые экраны, их назначение.
33. Способы реализации процесса балансировки нагрузки.
34. Способы размещения WEB и DNS серверов в сетевой инфраструктуре организации.
35. Прокси серверы и шлюзы и их назначение.
36. Виртуализация WEB и DNS серверов, организация кластеров.
37. Лицензии на межсетевых экранах и их применение. Настройка.
38. Настройка демилитаризованной зоны для веб сервера.
39. Способы борьбы с различными атаками на веб сервер.
40. Виды атак на веб серверы.
41. Оптимизация настроек сетевой карты для веб сервера и dns сервера.
42. Атаки на dns сервер.
43. Функция Dns relay и ее возможности на межсетевых экранах.
44. Механизм перенаправления трафика при обрыве канала связи.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОПК-8 – способностью использовать языки и системы программирования, инструментальные	**Знать:** устройство сети Интернет; языки разметки документов; протоколы http, https, ftp; принцип работы веб сервера; принципы функционирования веб	Практические работы по подгруппам, Билет к зачету, Билет к экзамену	Компетенции сформированы при правильности и полноте ответов на теоретические

	средства для решения профессиональных, исследовательских и прикладных задач.	приложений; средства разработки веб приложений; наиболее распространённые веб серверы, их возможности и функционал; способы создания простейших веб страниц; основные и дополнительные метатеги; способы создания и настройки дополнительных инструментариев, позволяющие увеличивать посещаемость сайтов; методы проверки и тестирования законченных сайтов; подходы к проектированию веб сервера и локально-вычислительной сети с сетевым оборудованием; способы защиты от различного рода сетевых атак на Web и DNS серверы, и сетевое оборудование; наиболее распространенные типы уязвимостей. **Уметь:** использовать средства разработки веб приложений; разрабатывать простые веб страницы на языке html; использовать основные и дополнительные метатеги; использовать дополнительный инструментарий, позволяющий увеличивать число посетителей и продвигать сайт в поисковых системах; настраивать веб сервер и его сетевые карты, роли DNS, IIS и другие для корректной работы сайта; настраивать межсетевые экраны, коммутаторы, балансировку нагрузки; организовывать серверные кластеры; производить анализ защищенности веб приложения; производить защиту веб приложения;		вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

		производить устранение основных типов угроз.		

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Сычев, А. В. Web-технологии : учебное пособие / А. В. Сычев. – 2-е изд. – Москва : ИНТУИТ, 2016. – 408 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/100725 (дата обращения: 15.05.2020). – Режим доступа: для авториз. пользователей.

7.2. Дополнительная литература:

1. Спецификация языка HTML : учебное пособие. – 2-е изд. – Москва : ИНТУИТ, 2016. – 489 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/100510 (дата обращения: 15.05.2020). – Режим доступа: для авториз. пользователей.
2. Основы работы с HTML : учебное пособие. – 2-е изд. — Москва : ИНТУИТ, 2016. – 208 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/100328 (дата обращения: 15.05.2020). – Режим доступа: для авториз. пользователей.

7.3. Интернет-ресурсы

1. Научная электронная библиотека. URL: http://elibrary.ru/.
2. Электронные ресурсы ИБЦ ТюмГУ. URL: https://bmk.utmn.ru/ru/.

7.4 Современные профессиональные базы данных и информационные справочные системы

- Межвузовская электронная библиотека (МЭБ). - URL: https://icdlib.nspu.ru/
- Национальная электронная библиотека. - URL: https://rusneb.ru/
- Institute of Electrical and Electronics Engineers, Inc (IEEE). - URL: https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- Orbit Intelligence. - URL: https://www.orbit.com

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Лицензионное ПО:
  - Microsoft Imagine Academy (ранее Dreamspark): ОС семейства MS Windows (редакция Pro/Server);
  - Офисный пакет Microsoft Office 365 (лицензионное соглашение №2т/00509-20 от 12.05.2020);
  - Платформа для электронного обучения Microsoft Teams.

- Свободно распространяемое ПО:
  - Программное обеспечение виртуализации: VirtualBox (бесплатная лицензия доступна: https://www.virtualbox.org/wiki/Downloads).

9. **Технические средства и материально-техническое обеспечение дисциплины (модуля)**

Учебные аудитории для проведения лекций и практических занятий;

Лаборатории, оснащенные лабораторным оборудованием в соответствии с ФГОС ВО 3+ по данному направлению.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

РАЗРАБОТКА И ЗАЩИТА МОБИЛЬНЫХ ПРИЛОЖЕНИЙ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Наурусова Г.А Разработка и защита мобильных приложений. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Разработка и защита мобильных приложений [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Наурусова Г.А, 2020.

1. Пояснительная записка

Разработка и защита мобильных приложений обеспечивает приобретение знаний и умений в соответствии с Федеральным государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Цель дисциплины «Разработка и защита мобильных приложений» - является изложение теоретических и практических принципов разработки и защиты мобильных приложений с учетом современных тенденций.

Задачи курса - изучение:

· устройства платформы Android
· системного подхода к проектированию и созданию мобильных приложений
· архитектуры мобильного приложения, основных его компонентов
· основ разработки интерфейсов мобильных приложений
· основ разработки многооконных приложений
· основ работы с базами данных SQLite
· предотвращения угроз безопасности мобильных приложений

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Вариативная часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Языки программирования», «Информатика», «Структуры и алгоритмы компьютерной обработки информации».

Дисциплина «Разработка и защита мобильных приложений» способствует освоению следующих дисциплин: «Администрирование и безопасность SQL Server».

1.2.**Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)**

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОПК-10 - способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах		Знать: виды и способы разграничения доступа к данным Уметь: реализовывать системы разграниченного доступа на практике
ОПК-7 - способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения		Знать: основные принципы работы устройства платформы Android Уметь: правильно определять и предотвращать основные угрозы для мобильных приложений
ОПК-8 - способность использовать языки и системы		Знать: основные принципы работы устройства платформы Android

программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач		Уметь: правильно определять и предотвращать основные угрозы для мобильных приложений
ПК-8 - способность участвовать в разработке подсистемы информационной безопасности компьютерной системы		Знать: основные принципы работы устройства платформы Android Уметь: правильно определять и предотвращать основные угрозы для мобильных приложений

* не предусмотрено

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)	
		9 семестр	10 семестр
Общий объем зач. ед.	**7**	3,5	3,5
час.	**252**	126	126
Из них:			
Часы аудиторной работы (всего):	**144**	72	72
Лекции	72	36	36
Практические занятия	0	0	0
Лабораторные/практические занятия по подгруппам	72	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	**108**	54	54
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет	экзамен

3. Система оценивания

3.1. К зачету допускаются студенты, набравшие за семестр 35 баллов. Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «зачет» студент должен сдать минимум 7 лабораторных работ в течение семестра или на зачете и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
Семестр						
1.	Введение в разработку мобильных приложений	12	4	4	4	0
2.	Виды мобильных приложений и их структура	12	4	4	4	0
3.	Основы архитектуры приложения, основных его компонентов	12	4	4	4	0
4.	Основы разработки интерфейсов мобильных приложений	12	4	4	4	0
5.	Основы разработки многооконных приложений	12	4	4	4	0
	Всего (часов) за семестр					0
Семестр						
6.	Использование возможностей смартфона в приложениях	12	4	4	4	0
7.	Основы работы с базами данных SQLite	12	4	4	4	0
8.	Новое поколение инструментальных средств разработки мобильных приложений	12	4	4	4	0
9.	Безопасность мобильных приложений	12	4	4	4	0
	Всего (часов) за семестр					0
	Итого (часов)	252	72	0	72	2

4.2. Содержание дисциплины (*модуля*) по темам

Модуль 1. Общие сведения.

1. Введение в разработку мобильных приложений. Основные принципы разработки для ОС Android. Устройство платформы Android. Обзор сред программирования для Android. Возможности отладки на эмуляторах и реальных устройствах.

2. Виды приложений и их структура. Особенности видов мобильных приложений. Организация исполнения приложений в ОС Android и каким образом обеспечивается безопасная среда их функционирования.

3. Основы архитектуры приложения, основных его компонентов. Активности (Activities). Сервисы (Services). Контент-провайдеры (Content providers).

Модуль 2. Основы разработки мобильных приложений.

4. Основы разработки интерфейсов мобильных приложений. Графический дизайн и пользовательские интерфейсы. Визуальный информационный дизайн. Обзор интерфейса.

5. Основы разработки многооконных приложений. Многооконные приложения. Работа с диалоговыми окнами. Особенности разработки приложения, содержащего несколько активностей.

6. Использование возможностей смартфона в приложениях. Отличительные особенности смартфонов. Сенсорное (touch) управление. Взаимодействие с системами позиционирования

Модуль 3.Комплексные мобильные приложения.

7. Основы работы с базами данных SQLite. Основы SQL.Типы данных. Операторы. Выражения. Практическое использование SQLite в мобильных приложениях. Создание базы данных и таблиц. Получение системных данных. Работа с данными в SQLite.

8. Новое поколение инструментальных средств разработки мобильных приложений. Обзор возможностей Intel XDK. Эмулятор и запуск на устройстве.

9. Безопасность мобильных приложений. Введение в безопасность мобильных приложений. Статистические данные угроз безопасности мобильных приложений. Методы обнаружения уязвимостей в мобильных приложениях. Метод тестирования на проникновение. Генерация запросов по шаблону с типизированными параметрами. Метод статического анализа. Метод динамического анализа. Уязвимости, приводящие к выполнению кода. Переполнение буфера. Атака на функции форматирования строк. Внедрение операторов LDAP. Выполнение команд операционной системы. Внедрение операторов SQL. Внедрение SQL кода вслепую. Внедрение серверных расширений.

Планы семинарских занятий.

Не предусмотрены

Темы практических работ с разделением на подгруппы.

1. Введение в разработку мобильных приложений.
2. Основы HTML, использование базовых тегов.
3. Основы CSS, верстка страниц.
4. Комплексное использование HTML и CSS.
5. Введение в PHP, написание фотогалереи.
6. Введение в SQLite, написание мобильного приложения для опубликования новостей.
7. Введение в SQLite, написание гостевой книги.
8. Регулярные выражения
9. Авторизация пользователя с помощью SQLite.
10. Система редактирования данных с разграничением прав доступа.

Примерная тематика курсовых работ.

Курсовых работ по предмету не предусмотрены.

Образцы средств для проведения текущего контроля: Практические работы с разделением на подгруппы.

Практическая работа с разделением на подгруппы № 1.

Установка Android Studio и написание простейшей программы «Hello World».

Практическая работа с разделением на подгруппы № 2.

Создание HTML страниц на основе представленных изображений.
Практическая работа с разделением на подгруппы № 3.
Расположить блоки с помощью HTML и CSS в заданном порядке.
Практическая работа с разделением на подгруппы № 4.
Сверстать с помощью HTML и CSS страницу из представленного изображения.
Практическая работа с разделением на подгруппы № 5.
Создать фотогалерею с помощью HTML, CSS, PHP. Подгрузку изображений организовать из подпапок, где каждая папка будет являться соответствующим разделом галереи.
Практическая работа с разделением на подгруппы № 6.
Создать мобильное приложение для опубликования новостей с помощью SQLite. Создать соответствующую базу данных и таблицу с новостями. Вывести новости списком, а также каждую новость подробнее. Новость должна содержать следующие поля:
Дата
Заголовок
Изображение
Краткое содержание
Подробное содержание
Практическая работа с разделением на подгруппы № 7.
Создать мобильное приложение - гостевая книга с помощью SQLite. Создать соответствующую базу данных и таблицу для гостевой книги. Выводить сообщения списком, а также реализовать возможность добавлять собственные сообщения пользователями. Сообщения в гостевой должны содержать следующие поля:
Имя
E-mail
Дата и время
Сообщение
Практическая работа с разделением на подгруппы № 8.
Реализовать регулярные выражения:
Практическая работа с разделением на подгруппы № 9.
Добавить к мобильному приложению из лабораторной работы №6 авторизацию пользователя. Создать соответствующую таблицу с пользователями, где каждый пользователь имеет следующие поля:
Псевдоним
Логин
Пароль, зашифрованный хеш функцией.
Практическая работа с разделением на подгруппы № 10.
Добавить к мобильному приложению из лабораторной работы №9 возможность изменять и добавлять новости только авторизованным пользователям, разграничить их права доступа к новостям.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
Семестр		
1.	Введение в разработку мобильных приложений	Конспектирование материала на лекционных занятиях. Дополнительно Работа с учебной литературой. Выполнение расчетной работы, выполнение практических работ.
2.	Виды мобильных приложений и их структура	Конспектирование материала на лекционных занятиях. Дополнительно Работа с учебной

		литературой. Выполнение расчетной работы, выполнение практических работ.
3.	Основы архитектуры приложения, основных его компонентов	Конспектирование материала на лекционных занятиях. Дополнительно Работа с учебной литературой. Выполнение расчетной работы, выполнение практических работ.
4.	Основы разработки интерфейсов мобильных приложений	Конспектирование материала на лекционных занятиях. Дополнительно Работа с учебной литературой. Выполнение расчетной работы, выполнение практических работ.
5.	Основы разработки многооконных приложений	Конспектирование материала на лекционных занятиях. Дополнительно Работа с учебной литературой. Выполнение расчетной работы, выполнение практических работ.
Семестр		
6.	Использование возможностей смартфона в приложениях	Конспектирование материала на лекционных занятиях. Дополнительно Работа с учебной литературой. Выполнение расчетной работы, выполнение практических работ.
7.	Основы работы с базами данных SQLite	Конспектирование материала на лекционных занятиях. Дополнительно Работа с учебной литературой. Выполнение расчетной работы, выполнение практических работ.
8.	Новое поколение инструментальных средств разработки мобильных приложений	Конспектирование материала на лекционных занятиях. Дополнительно Работа с учебной литературой. Выполнение расчетной работы, выполнение практических работ.
9.	Безопасность мобильных приложений	Конспектирование материала на лекционных занятиях. Дополнительно Работа с учебной литературой. Выполнение расчетной работы, выполнение практических работ.

Порядок выполнения каждого вида самостоятельной работы:

Для подготовки практических работ необходимо пользоваться конспектом лекций и [1,2] из списка основной литературы. Для получения расширенных и углубленных знаний по тематике рекомендуется пользоваться ссылками из списка интернет-ресурсов, приведенных в данном УМК, а также электронными и бумажными номерами научных журналов, имеющихся в ИБЦ, областной научной библиотеке и сети интернет

6. .Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения экзамена – контрольная работа.

Вопросы к зачету

1. Введение в разработку мобильных приложений. Основные принципы разработки для ОС Android. Устройство платформы Android.

2. Обзор сред программирования для Android. Возможности отладки на эмуляторах и реальных устройствах.

3. Виды приложений и их структура. Особенности видов мобильных приложений.

4. Организация исполнения приложений в ОС Android и каким образом обеспечивается безопасная среда их функционирования.

5. Основы архитектуры приложения, основных его компонентов. Активности (Activities).
6. Основы архитектуры приложения, основных его компонентов. Сервисы (Services).
7. Основы архитектуры приложения, основных его компонентов. Контент-провайдеры (Content providers).
8. Основы разработки интерфейсов мобильных приложений. Графический дизайн и пользовательские интерфейсы.
9. Основы разработки интерфейсов мобильных приложений. Визуальный информационный дизайн. Обзор интерфейса.
10. Основы разработки многооконных приложений. Многооконные приложения. Работа с диалоговыми окнами.
11. Особенности разработки приложения, содержащего несколько активностей.
12. Использование возможностей смартфона в приложениях. Отличительные особенности смартфонов. Сенсорное (touch) управление.
13. Взаимодействие с системами позиционирования.
14. Основы работы с базами данных SQLite. Практическое использование SQLite в мобильных приложениях. Создание базы данных и таблиц. Получение системных данных.
15. Новое поколение инструментальных средств разработки мобильных приложений. Обзор возможностей Intel XDK. Эмулятор и запуск на устройстве.
16. Безопасность мобильных приложений. Введение в безопасность мобильных приложений. Статистические данные угроз безопасности мобильных приложений. Методы обнаружения уязвимостей в мобильных приложениях. Метод тестирования на проникновение. Генерация запросов по шаблону с типизированными параметрами. Метод статического анализа. Метод динамического анализа.
17. Виды уязвимостей. Уязвимости, приводящие к выполнению кода. Переполнение буфера. Атака на функции форматирования строк. Внедрение операторов LDAP. Выполнение команд операционной системы. Внедрение операторов SQL. Внедрение SQL кода вслепую. Внедрение серверных расширений.

6.2.Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОПК-10 - способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Знать виды и способы разграничения доступа к данным Уметь реализовывать системы разграниченного доступа на практике	Опрос на практическом занятии, выполнение практических заданий, зачет	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев
2.	ОПК-7 - способность учитывать современные тенденции развития	Знать основные принципы работы сети Интернет Уметь правильно определять и предотвращать основные угрозы для программ в Интернете	Опрос на практическом занятии, выполнение практически	

	информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения		х заданий, зачет	применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
3.	ОПК-8 - способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Знать основные принципы работы сети Интернет Уметь правильно определять и предотвращать основные угрозы для программ в Интернете	Опрос на практическом занятии, выполнение практических заданий, зачет	
4.	ПК-8 - способность участвовать в разработке подсистемы информационной безопасности компьютерной системы	Знать виды и способы защиты информации при разработке WEB приложений Уметь находить уязвимые места в коде WEB приложения и устранять их	Опрос на практическом занятии, выполнение практических заданий, зачет	

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература:

1. Пирская Л.В. Разработка мобильных приложений в среде Android Studio : учебное пособие / Л. В. Пирская. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2019. — 123 с. — ISBN 978-5-9275-3346-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/100196.html (дата обращения: 25.05.2020). — Режим доступа: для авторизир. пользователей

7.2 Дополнительная литература:

1. Введение в разработку приложений для ОС Android : учебное пособие / Ю. В. Березовская, О. А. Юфрякова, В. Г. Вологдина, О. В. Озерова. — 2-е изд. — Москва : ИНТУИТ, 2016. — 433 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100707 (дата обращения: 25.05.2020). — Режим доступа: для авториз. пользователей.

7.3 Интернет-ресурсы:

1. Основы Kotlin. https://www.fandroid.info/osnovy-kotlin-vvedenie/
2. Единое окно доступа к образовательным ресурсам http://window.edu.ru/

3. Национальный открытый университет «ИНТУИТ» http://www.intuit.ru/

7.4 Современные профессиональные базы данных и информационные справочные системы:

Institute of Electrical and Electronics Engineers, Inc (IEEE). URL: https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true.

Межвузовская электронная библиотека (МЭБ). URL: https://icdlib.nspu.ru/.

Национальная электронная библиотека. URL: https://rusneb.ru/.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- платформа для электронного обучения Microsoft Teams.

Интернет, доступ в информационно-образовательную среду ТюмГУ, включающую в себя доступ к учебным планам и рабочим программам, к изданиям электронной библиотечной системы и электронным образовательным ресурсам, Android Studio

9. **Технические средства и материально-техническое обеспечение дисциплины (модуля)**

Учебные аудитории для проведения занятий лекционного и практического типа, консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы. Для проведения занятий лекционного типа необходимо демонстрационное оборудование. Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Захаров А.А. Сети и системы передачи информации. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Сети и системы передачи информации [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Захаров А.А., 2020.

1. Пояснительная записка

Дисциплина «Сети и системы передачи информации» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Цель дисциплины «Сети и системы передачи информации» – изучение методов и средств построения и эксплуатации программно-аппаратных технологий, изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию технологий передачи информации.

Задачи курса – изучение:

- принципов построения, функционирования и применения аппаратных средств современной вычислительной техники;
- основных теоретических концепций, положенных в основу построения современных компьютеров, вычислительных систем, сетей и телекоммуникаций.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Математический анализ», «Информатика».

Дисциплина «Сети и системы передачи информации» способствует освоению следующих дисциплин: «Аппаратные средства вычислительной техники».

1.2.**Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)**

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-8 - способность к самоорганизации и самообразованию		знать: - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; уметь: - самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;
ПК-10 - способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы		Знает: протоколы передачи информации; Умеет: применять полученные знания к различным предметным областям.

управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		
ПК-5 - способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		Знает: основные угрозы, способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах. Умеет: классифицировать и оценивать угрозы безопасности информации; определять подлежащие защите информационные активы автоматизированных систем.

* не предусмотрено

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)	
		3 семестр	**4** семестр
Общий объем зач. ед.	8	4	4
час.	288	144	144
Из них:			
Часы аудиторной работы (всего):	144	72	72
Лекции	72	36	36
Практические занятия	0	0	0
Лабораторные/практические занятия по подгруппам	72	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	144	72	72
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет	экзамен

3. Система оценивания

3.1. В соответствии с балльно-рейтинговой системой, принятой в ТюмГУ, оценку «удовлетворительно» получают студенты, набравшие за семестр не менее 61 балла, «хорошо» - 76, «отлично» - 91. Для зачета достаточно набрать 61 балл и более. В случае, если оценка не устраивает студента, или если он не набрал 61 балл, он может сдать экзамен. К экзамену допускаются студенты, набравшие за семестр 35 баллов. Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса и 1 задание. Для получения оценки «удовлетворительно» студентом должно быть сдано практическое задание и сделан ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок.

Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен сдать практическое задание и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности, может воспроизвести общую схему описываемого протокола или технологии, знает и понимает основные свойства, слабости и область применения протокола. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты, допускается отсутствие подробного описания транзакций протоколов, если приведена их суть. Для получения оценки «отлично» студент должен сдать практическое задание и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. В ответе должны быть приведено подробное описание транзакций протоколов с пояснением цели каждой из них.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
Семестр 3						
1.	Введение.	16	4	0	4	0
2.	Коммуникации с помощью сетей.	16	4	0	4	0
3.	Модель OSI. Уровень приложений и транспортный уровень.	16	4	0	4	0
4.	Сетевой уровень модели OSI.	16	0	0	4	0
5.	Адресация в сети – IPv4.	16	4	0	4	0
6.	Канальный и физический уровень модели OSI.	16	4	0	4	0
7.	Ethernet.	16	4	0	4	0
8.	Планирование и монтаж сети.	16	4	0	4	0
9.	Конфигурирование и тестирование сети.	16	4	0	4	0
	Всего (часов) за семестр 3	144	36	0	36	0

Семестр 4						
10.	Статическая маршрутизация.	16	4	0	4	0
11.	Динамическая маршрутизация.	16	4	0	4	0
12.	Дистанционно-векторные протоколы маршрутизации.	16	4	0	4	0
13.	RIP, VLSM и CIDR.	16	4	0	4	0
14.	RIPv2.	16	4	0	4	0
15.	Таблицы маршрутизации.	16	4	0	4	0
16.	EIGRP.	16	4	0	4	0
17.	Протоколы маршрутизации по состоянию канала.	16	4	0	4	0
18.	OSPF.	16	4	0	4	0
	Всего (часов) за семестр 4	144	36	0	36	0
	Итого (часов)	288	72		72	2

4.2. Содержание дисциплины (*модуля*) по темам

Модуль 1

1. Введение.

Коммуникации в мире с развитыми сетевыми технологиями. Современное состояние и перспективы коммуникаций. Компьютерные сеть как платформа Архитектура Интернет. Направления в развитии сетей.

2. Коммуникации с помощью сетей.

Платформа для коммуникаций. LAN, WAN и Интернет. Протоколы. Использование уровневых моделей. Сетевая адресация.

3. Модель OSI. Уровень приложений и транспортный уровень.

Функции уровня приложений модели OSI. Обеспечение приложений и служб. Примеры протоколов и служб уровня приложения. Транспортный уровень модели OSI. Функции транспортного уровня. TCP протокол – надежное соединение. Управление сессиями TCP. Протокол UDP – соединение с низкими накладными расходами.

Модуль 2.

4. Сетевой уровень модели OSI.

IPv4. Деление устройств на группы. Маршрутизация – как управляются пакеты данных. Процесс маршрутизации.

5. Адресация в сети – IPv4.

IPv4 адреса. Адреса различного назначения. Назначение адресов Идентификация сети. Вычисление адресов. Тестирование сетевого уровня.

6. Канальный и физический уровни модели OSI.

Канальный уровень. Методы доступа к среде. Адресация и деление данных на кадры в подуровне доступа к среде. Физический уровень модели OSI. Коммуникационные сигналы. Физическая передача сигналов и кодирование: представление данных. Среда передачи данных.

Модуль 3.

7. Ethernet.

Ethernet – соединение через LAN 3. Кадр Ethernet. Контроль доступа к среде в Ethernet. Физический уровень Ethernet. Концентраторы и коммутаторы. Протокол разрешения адресов (ARP).

8. Планирование и монтаж сети.

LAN – физическое соединение. Соединение устройств. Разработка адресной схемы. Расчет подсетей.

9. Конфигурирование и тестирование сети.

Конфигурирование устройств Cisco – основы IOS. Применение базовой конфигурации с помощью Cisco IOS. Проверка соединения. Отслеживание и документирование сетей.

Модуль 4.

10. Статическая маршрутизация.

Протоколы маршрутизации и перенаправление пакетов. CLI конфигурация и адресация. Построение таблицы маршрутизации. Функции определения пути и коммутации. Статическая маршрутизация. Маршрутизаторы в сетях. Обзор конфигурации маршрутизатора. Обнаружение подключенных сетей. Статические маршруты с «NextHop» адресами. Статические маршруты с выходными интерфейсами. Суммарный маршрут и маршрут по умолчанию. Поддержка и исправления статических маршрутов.

11. Динамическая маршрутизация.

Классификация динамических протоколов маршрутизации. Метрики. Административные дистанции. Сабнеттинг.

12. Дистанционно-векторные протоколы маршрутизации.

Обнаружение сетей. Поддержка таблицы маршрутизации. Маршрутные петли. Дистанционно-векторные протоколы маршрутизации в настоящее время.

Модуль 5.

13. RIP, VLSM и CIDR.

RIP версии 1: дистанционно векторный, классовый протокол маршрутизации. Основы конфигурирования RIPv1. Обнаружение и исправление ошибок. Автоматическая суммаризация. Маршрут по умолчанию и RIPv1. VLSM и CIDR. Классовая и бесклассовая адресация. VLSM и суммаризация маршрутов.

14. RIPv2.

Ограничения RIPv1. Конфигурирование RIPv2. VLSM и CIDR. Обнаружение и исправление ошибок в RIPv2.

15. Таблицы маршрутизации.

Структура таблицы маршрутизации. Процесс просмотра таблицы маршрутизации. Процесс маршрутизации.

Модуль 6.

16. EIGRP.

Основы конфигурации EIGRP. Подсчет метрики EIGRP. DUAL. Расширенная конфигурация EIGRP.

17. Протоколы маршрутизации по состоянию канала.

Внедрение протоколов маршрутизации по состоянию канала.

18. OSPF.

Основы конфигурации OSPF. Метрика OSPF. OSPF и сети со множественным доступом. Расширенное конфигурирование OSPF.

6. Планы семинарских занятий.

Не предусмотрены.

7. Темы лабораторных работ (Лабораторный практикум).

Модуль 1.
1. LAN и WAN.
2. Уровень приложений.
3. Транспортный уровень.

Модуль 2.
4. Адресация в сети.
5. Канальный уровень модели OSI.
6. Физический уровень модели OSI.

Модуль 3.
7. Планирование сети.
8. Конфигурирование и тестирование сети.
9. Лабораторный практикум: конфигурация маршрутизатора.

Модуль 4.
10. Лабораторный практикум: конфигурирование статических маршрутов
11. Практика по протоколам маршрутизации и сабнеттингу.
12. Практические занятия по дистанционно-векторным протоколам маршрутизации.

Модуль 5.
13. Практические занятия по RIPv1.
14. Практические занятия по VLSM и суммаризации маршрутов.
15. Лабораторный практикум: конфигурирование RIPv2.

Модуль 6.
16. Таблицы маршрутизации.
17. Лабораторный практикум: конфигурирование EIGRP.
18. Лабораторный практикум: конфигурирование OSPF

8. Примерная тематика курсовых работ.
Курсовые работы (проекты) по данной дисциплине не предусмотрены.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Введение.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
2.	Коммуникации с помощью сетей.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
3.	Модель OSI. Уровень приложений и транспортный уровень.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
4.	Сетевой уровень модели OSI.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.

5.	Адресация в сети – IPv4.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
6.	Канальный и физический уровень модели OSI.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
7.	Ethernet.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
8.	Планирование и монтаж сети.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
9.	Конфигурирование и тестирование сети.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
10.	Статическая маршрутизация.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
11.	Динамическая маршрутизация.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
12.	Дистанционно-векторные протоколы маршрутизации.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
13.	RIP, VLSM и CIDR.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
14.	RIPv2.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
15.	Таблицы маршрутизации.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
16.	EIGRP.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
17.	Протоколы маршрутизации по состоянию канала.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.
18.	OSPF.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы.

Порядок выполнения каждого вида самостоятельной работы:

1. Конспектирование материала на лекционных занятиях.
2. Работа с учебной литературой.
3. Выполнение лабораторной работы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации в 3 семестре – зачет.

Вопросы к зачету

1. Локальные LAN, глобальные WAN и объединенные сети
2. Архитектура сети Интернет
3. Использование модели уровней
4. Примеры протоколов и сервисов прикладного уровня
5. Протокол управления передачей TCP – надежная коммуникация
6. Протокол дейтаграмм пользователя UDP – коммуникация с малой нагрузкой
7. IPv4
8. Маршрутизация – как обрабатываются наши пакеты
9. Процесс маршрутизации: как узнаются маршруты
10. Адресация IPv4
11. Вычисление адресов
12. Канальный уровень – Доступ к среде передачи
13. Адресация при доступе к среде и формирование кадров
14. Физический уровень – коммуникация сигналов
15. Ethernet – коммуникации через локальную сеть
16. Кадр Ethernet
17. Хабы и свитчи
18. Протокол разрешения адресов ARP
19. Настройка устройств Cisco – Основы IOS
20. Применение базовых настроек используя Cisco IOS

Форма проведения промежуточной аттестации в 4 семестре – экзамен.

Вопросы к экзамену

1. Внутренности маршрутизатора
2. Создание таблицы маршрутизации
3. Выбор маршрута и функции коммутации
4. Исследование непосредственно подключенных сетей
5. Статические маршруты с адресом «следующего прыжка»
6. Статические маршруты с указанием выходного интерфейса
7. Суммированный маршрут и маршрут по умолчанию
8. Классификация динамических протоколов маршрутизации
9. Метрики
10. Административные расстояния
11. RIPv1: Дистанционно-векторный, классовый протокол маршрутизации
12. Базовая настройка RIPv1
13. Классовая и бесклассовая адресация
14. VLSM и CIDR
15. Ограничения RIPv1
16. Настройка RIPv2
17. Структура таблицы маршрутизации
18. Процесс поиска в таблице маршрутизации
19. Базовая настройка EIGRP

20. Вычисление метрики EIGRP
21. Дополнительная настройка EIGRP
22. Базовая настройка OSPF
23. Метрика в OSPF
24. Дополнительная настройка OSPF

Тестирование и материалы к лабораторным работам находятся на ресурсе cisco.netacad.com, дополнительно материал к лабораторным работам издан в виде учебно-методических пособий (Бабич,А.В. Организация информационных сетей: учеб. пособие/ А. В. Бабич; Тюм. гос. ун-т. - Тюмень: Изд-во ТюмГУ, 2010. - 144 с.; 20 см. - Библиогр. : с. 142.; Бабич, А. В.Сетевые технологии: учеб.пособие/ А. В. Бабич; Тюм. гос. ун-т. -Тюмень: Изд-во ТюмГУ, 2010. - 156 с.; 20 см. - Библиогр.: с. 155.), хранящихся на кафедре информационной безопасности.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОК-8 - способность к самоорганизации и самообразованию	знать: - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; уметь: - самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;	Лабораторная работа, задание для зачета, экзаменационные билеты	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся

				ФГАОУ ВО ТюмГУ»
1.	ПК-10 - способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает: протоколы передачи информации; Умеет: применять полученные знания к различным предметным областям.	Лабораторная работа, задание для зачета, экзаменационные билеты	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-5 - способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает: основные угрозы, способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах. Умеет: классифицировать и оценивать угрозы безопасности информации; определять подлежащие защите информационные активы автоматизированных систем.	Лабораторная работа, задание для зачета, экзаменационные билеты	

* - не предусмотрен

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Сети связи и системы коммутации: Учебное пособие / Паринов А.В., Ролдугин С.В., Мельник В.А. - Воронеж:Научная книга, 2016. - 178 с. ISBN 978-5-4446-0906-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/923309 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

7.2. Дополнительная литература:

− 1. Нужнов Е.В. Компьютерные сети. Часть 2. Технологии локальных и глобальных сетей : учебное пособие / Нужнов Е.В.. — Таганрог : Издательство Южного федерального университета, 2015. — 176 с. — ISBN 978-5-9275-1691-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/78675.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. Пользователей.

− 2. Чернецова Е.А. Системы и сети передачи информации. Часть 1. Системы передачи информации / Чернецова Е.А.. — Санкт-Петербург : Российский государственный гидрометеорологический университет, 2008. — 203 с. — ISBN 978-5-86813-204-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/17966.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

3. Чернецова Е.А. Системы и сети передачи информации. Часть 2. Сети передачи информации / Чернецова Е.А.. — Санкт-Петербург : Российский государственный гидрометеорологический университет, 2008. — 199 с. — ISBN 978-5-86813-207-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/17967.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

7.3. Интернет-ресурсы

1. учебный центр cisco.netocad.com для проведения тестов и проверки знаний.
2. Авторизованные курсы по сетевым технологиям:
    1. CCNA Exploration 1: Network Fundamentals Tyumen State University. Режим доступа: https://1404116.netacad.com/courses/78983/assignments/1567605
    2. CCNA R&S: Routing Protocols Tyumen State University. Режим доступа: https://1404116.netacad.com/courses/98158

7.4 Современные профессиональные базы данных и информационные справочные системы:

https://www.utmn.ru/obrazovanie/normativnye-dokumenty/akkteditatsiya/dokumenty-tyumgu/.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Cisco Packet Tracer.
- среда для электронного обучения MS Teams

9. **Технические средства и материально-техническое обеспечение дисциплины (модуля)**

Компьютерный класс с выходом в интернет и стандартное лабораторное и периферийное оборудование классом не ниже чем в приведенной ниже конфигурации:

- 3 маршрутизатора Cisco 2801 с Base IP IOS, 128 Мбайт DRAM, 32 Мбайта флэш-памяти и модулями HWIC-2A/S;
- 3 коммутатора Cisco Catalyst 2960;
- Набор последовательных кабелей (входят в комплект поставки оборудования для Сетевой академии);

- 2 беспроводных маршрутизатора Linksys (предпочтительно Linksys WRT150N, допустимо использование моделей WRT54G, WRT300N и WRT350N) или аналогичные устройства SOHO.

Для проведения лекционных и практических занятий необходим проектор с разрешением не менее 800x1200, подключенный к компьютеру с выходом в Интернет.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Нестерова О.А Системы управления базами данных. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Системы управления базами данных [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Нестерова О.А, 2020.

1. Пояснительная записка

Системы управления базами данных базами данных даёт общее представления о системе управления базами данных как об одной из основных составляющих эффективных систем автоматизированной обработки информации. Изучаются характеристики и типы систем баз данных, области применения систем управления базами данных, этапы проектирования баз данных, логическую организацию реляционной баз данных, средства поддержания целостности в реляционной модели, а также приводится методика составления запросов для работы с данными и метаданными БД, используя структурированный язык запросов.

Цель дисциплины «Системы управления базами данных» - формирование у студентов совокупности профессиональных качеств, обеспечивающих решение проблем, связанных с проектированием и реализацией прикладных защищенных решений и баз данных под управлением современных систем управления базами данных (СУБД).

Задачи курса -

- обучить студентов принципам работы современных систем управления базами данных;
- привить студентам навыки проектирования и реализации баз данных;
- дать студентам представление о проектировании и эксплуатации реляционных баз данных.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Языки программирования», «Информатика».

Дисциплина «Системы управления базами данных» способствует освоению следующих дисциплин: «Разработка защищенных прикладных решений на базе современных систем управления базами данных», «Разработка и эксплуатация информационных систем в защищенном исполнении», «Безопасность систем баз данных».

1.2.**Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)**

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-8 - способность к самоорганизации и самообразованию		***знать:*** - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; ***уметь:*** - самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;
ПК-10 - способность оценивать эффективность реализации систем защиты информации и		***Знать:*** области применения систем управления базами данных;

действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		особенности управления данными в системах распределенной обработки; работы с системами управления базами данных на различных платформах; ***Уметь:*** разрабатывать программы на высокоуровневых языках программирования; применять навыки разработчика и администратора баз данных

* не предусмотрено

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		4 семестр
Общий объем зач. ед.	3	3
час.	108	108
Из них:		
Часы аудиторной работы (всего):	72	72
Лекции	36	36
Практические занятия	0	0
Лабораторные/практические занятия по подгруппам	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	36	36
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет

3. Система оценивания

3.1. Для текущего контроля применяется 100-балльная система оценивания. Баллы проставляются за посещение практических занятий и активную работу на них, а также за выполненные практические работы по каждой теме дисциплины. Результаты текущего контроля учитываются при промежуточной аттестации. Перевод баллов осуществляется по следующей шкале: от 61 – «зачтено»; менее 61 балла – «незачтено». Обучающиеся, не набравшие достаточного количества баллов для оценки, сдают зачет в период зачетной недели. Форма проведения зачета – собеседование. Продолжительность выполнения - астрономический час.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п		**Объем дисциплины (модуля), час.**		
		Всего	**Виды аудиторной работы** (академические часы)	**Иные виды**

	Наименование тем и/или разделов		Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	контактной работы
1	2	3	4	5	6	7
1.	История развития, назначение и роль баз данных. Этапы развития информационных систем	5	2	0	0	0
2.	Общие принципы построения БД. Модели данных	5	2	0	2	0
3.	Основы построения реляционных БД.	8	2	0	2	0
4.	Физическая организация баз данных	10	2	0	2	0
5.	Нормализация базы данных	10	4	0	4	0
6.	Языковые средства СУБД для различных моделей данных. Язык SQL	10	4	0	4	0
7.	Планирование, проектирование и администрирование БД	10	4	0	4	0
8.	Сервисные средства СУБД. Средства автоматизации проектирования баз данных	10	4	0	4	0
9.	Средства поддержания целостности базы данных.	10	4	0	4	0
10.	Эксплуатация баз данных	10	4	0	4	0
11	Технология и модели архитектуры клиент/сервер. Серверы баз данных.	10	4	0	4	
12	Типология БД	10	2	0	2	
	Итого (часов)	108	36	0	36	0

4.2. Содержание дисциплины (*модуля*) по темам

1. История развития, назначение и роль баз данных. Этапы развития информационных систем. Информация и данные. Базы данных и файловые системы. Функции и состав СУБД. Ранние подходы к организации БД. Понятие базы данных. Файловые системы и системы с базами данных. Компоненты СУБД. Распределение обязанностей в системах с базами данных. Администраторы данных и баз данных, разработчики баз данных, прикладные программисты, пользователи. Классификация задач, решаемых с использованием СУБД.

2. Общие принципы построения БД. Модели данных. Общая характеристика, назначение и возможности, классификация, состав и архитектура СУБД. Информационное, лингвистическое, математическое, аппаратное, организационное, правовое обеспечения СУБД. Отображение предметной области. Сущности и связи. Методы абстрагирования данных. Иерархическая, сетевая, реляционная модели данных. Трехуровневая архитектура ANSI-SPARC. Внешний уровень. Концептуальный уровень. Внутренний уровень.
3. Основы построения реляционных БД. История реляционной модели. Реляционная модель. Терминология. Структура реляционных данных. Реляционные ключи. Реляционная целостность. Реляционная алгебра. Реляционное исчисление. Представления.
4. Физическая организация баз данных. Структуры данных и базы данных. Способы хранения информации в базах данных. Способы повышения эффективности обработки данных за счет их организации.
5. Нормализация базы данных. Аномалии при эксплуатации баз данных. Нормальные формы БД. Денормализация.
6. Языковые средства СУБД для различных моделей данных. Язык SQL. Языковые средства манипулирования данными в реляционных СУБД. Языковые средства описания данных реляционных СУБД. Хранимые процедуры. Работа с триггерами и управление транзакциями
7. Планирование, проектирование и администрирование БД. Жизненный цикл приложения баз данных. Этапы жизненного цикла приложения БД. Обзор процедуры проектирования БД. Проектирование приложений. Выбор СУБД. особенности средств управления в реализациях реляционных СУБД. Администрирование.
8. Сервисные средства СУБД; средства автоматизации проектирования баз данных. Общая характеристика, назначение и возможности, классификация, универсальные и специализированные генераторы программ для СУБД; перспективы развития СУБД.
9. Средства поддержания целостности базы данных. Метаданные. Словарь-справочник данных. Ограничения целостности. Ссылочная целостность. 7 Механизм транзакций. Проблемы оптимизации доступа к базам данных. Средства дублирования и восстановления. Особенности реализации БД с высокими требованиями на надежность хранения и обработки.
10. Эксплуатация баз данных. Организация процессов обработки данных в БД. Состав, порядок планирования и проведения регламентных работ. Сервисные средства СУБД. Задачи администратора базы данных. Организация труда обслуживающего персонала. Средства реализации диалогового интерфейса и подготовки отчетов в языках СУБД.
11. Технология и модели архитектуры клиент/сервер. Серверы баз данных. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД. Использование средств прямого ввода-вывода, управления памятью, поддержания целостности, защиты от сбоев. Технология оперативной обработки транзакции (OLTP–технология). Поддержка Internet-технологий. Оценка эффективности и адаптации функционирования сервера баз данных. Проблемы оптимизации доступа к базе данных. Перспективы развития СУБД.
12. Типология БД: Документальные БД. Фактографические БД. Гипертекстовые и мультимедийные БД. XML-серверы. Объектноориентированные БД. Коммерческие БД. Распределенные БД в сетях ЭВМ.

Тема 2: Общие принципы построения БД. Модели данных.

1. Файловая система

2. Знакомство с MS Access.

Тема 3: Основы построения реляционных БД.

3. Работа со связанными таблицами Создание базы данных Study.

4. Общие принципы построения БД

Тема 4: Физическая организация баз данных.

5. Экспорт в другую СУБД

Тема 5: Нормализация базы данных.

6. Логическое проектирование

7. Нормализация БД. Этап 1

Тема 6: Языковые средства СУБД для различных моделей данных. Язык SQL.

8. Нормализация БД. Этап 2

Тема 7: Планирование, проектирование и администрирование БД.

Тема 9: Средства поддержания целостности базы данных.

9. Создание физической модели данных.

Тема 10: Эксплуатация баз данных.

10. Составление запросов на языке SQL. Создание представлений**.**

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	История развития, назначение и роль баз данных. Этапы развития информационных систем	Конспектирование материала на лекционных занятиях. Выполнение практической работы с разделением на подгруппы. Работа с учебной литературой. Подготовка собеседованию.
2.	Общие принципы построения БД. Модели данных	Конспектирование материала на лекционных занятиях. Выполнение практической работы с разделением на подгруппы. Работа с учебной литературой. Подготовка собеседованию.
3.	Основы построения реляционных БД	Конспектирование материала на лекционных занятиях. Выполнение практической работы с разделением на подгруппы. Работа с учебной литературой. Подготовка собеседованию.
4.	Физическая организация баз данных	Конспектирование материала на лекционных занятиях. Выполнение практической работы с разделением на подгруппы. Работа с учебной литературой. Подготовка собеседованию
5.	Нормализация базы данных	Конспектирование материала на лекционных занятиях. Выполнение практической работы с разделением на подгруппы. Работа с учебной литературой. Подготовка собеседованию.
6.	Языковые средства СУБД для различных моделей данных. Язык SQL	Конспектирование материала на лекционных занятиях. Выполнение практической работы с разделением на подгруппы. Работа с учебной литературой. Подготовка собеседованию.
7.	Планирование, проектирование и администрирование БД	Конспектирование материала на лекционных занятиях. Выполнение практической работы с разделением на подгруппы. Работа с учебной литературой. Подготовка собеседованию.
8.	Сервисные средства СУБД. Средства автоматизации проектирования баз данных	Конспектирование материала на лекционных занятиях. Выполнение практической работы с разделением на подгруппы. Работа с учебной литературой. Подготовка собеседованию.

9.	Средства поддержания целостности базы данных.	Конспектирование материала на лекционных занятиях. Выполнение практической работы с разделением на подгруппы. Работа с учебной литературой. Подготовка собеседованию.
10.	Эксплуатация баз данных	Конспектирование материала на лекционных занятиях. Выполнение практической работы с разделением на подгруппы. Работа с учебной литературой. Подготовка собеседованию.
11	Технология и модели архитектуры клиент/сервер. Серверы баз данных.	Конспектирование материала на лекционных занятиях. Выполнение практической работы с разделением на подгруппы. Работа с учебной литературой. Подготовка собеседованию.
12	Типология БД	Конспектирование материала на лекционных занятиях. Выполнение практической работы с разделением на подгруппы. Работа с учебной литературой. Подготовка собеседованию.

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме
2. Изучение рекомендованной основной и дополнительной литературы
3. Ответы на пункты плана для практических занятий
4. Разбор практических примеров, продемонстрированных на лекциях и решенных на практических занятиях

Контроль за самостоятельной работой осуществляется при выполнении обучающимся теста, контрольной работы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения зачета – контрольная работа.

Вопросы к зачету

1.Основные понятия ИС и БД. Особенности организации данных в БД. Определение ИС, составляющие ИС, примеры. Характеристика каждой составляющей ИС. Определение предметной области. Информационное обеспечение ИС (определение, примеры). Определение БД.
2.Определение БД. Ограничения, присущие традиционным файловым системам. Особенности организации данных в БД. Требования к БД со стороны внешних пользователей.
3.SQL. Определение, назначение. История создания. Стандарты и расширения. Transact SQL. Операторы защиты и управления данными (определения и перечислить).
4.SQL. Команды DDL. Назначение, определение. Перечислить все команды DDL, описать синтаксис и назначение, привести примеры.
5.SQL. Команды DML. Назначение, определение. Перечислить все команды DML, описать синтаксис и назначение, привести примеры.
6.SQL. Оператор SELECT. Определение, назначение, синтаксис, состав, возможности, примеры.
7.SQL. Особенности использования JOIN в SELECT. Определение, назначение, синтаксис, виды, примеры.

8.SQL. Оператор WHERE. Определение, назначение и все виды используемых в нем предикатов. Примеры. Особенности обработки NULL-значений.
9.SQL. Команды вставки, изменения удаления данных. Определение, назначение, примеры.
10.SQL. GROUP BY. Определение, назначение, примеры. Агрегирующие функции, условие для сгруппированных записей. Особенности использования агрегирующих функций.
11.Этапы проектирования БД. Основные понятия понятия, определения, особенности каждого этапа. Последовательность. Особенности перехода от одного этапа к следующему.
12.Инфологическая модель данных. Назначение. Определения всех элементов, их характеристики. Моделирование ограничений.
13.Ловушки соединения. Проблемы и основные принципы ER-моделирования. Виды, определения примеры ловушек (через семантические сети). Перечислить и пояснить основные принципы ER-моделирования.
14.Логическая (даталогическая) модель базы данных. Назначение. Определение всех элементов и их характеристики. Переход от ER-модели к логической. Проблемы.
15.Компоненты даталогической модели данных. Иерархическая и сетевая модели данных. Определения, примеры. Способы и операции определения, модификации и обеспечения целостности данных.
16.Реляционная модель данных. Назначение, определение, примеры. Описание основных элементов. Способы и операции определения, модификации и обеспечения целостности данных. Виды целостности данных. Достоинства и недостатки.
17.Реляционная алгебра. Теоретико-множественные операции. Определение, назначение, примеры всех теоретико-множественных операций. Определение отношений, совместимых по типу.
18.Реляционная алгебра. Специальные реляционные операции. Определение, назначение, примеры всех специальных операций.
19.Нормализация. 1НФ - 3НФ. Определения: нормализации, однозначной функциональной зависимости, транзитивной функциональной зависимости, нормальных форм. Правила и принципы нормализации. Декомпозиция отношений. Цель нормализации. Плюсы и минусы приведения БД к 3НФ.
20.Нормализация НФБК - 5НФ. Определения: денормализации, многозначной функциональной зависимости, функциональной зависимости соединения, нормальной формы, избыточности, аномалий. Правила и принципы нормализации. Плюсы и минусы приведения БД к 5НФ.
21.Этапы проектирования БД (основные понятия). Инфологический и даталогический аспекты. Определение и задачи каждого этапа. Определение соответствующих моделей. Критерии оценки эффективности моделей.
22.Физическая модель базы данных. Ключи (первичные, возможные потенциальные, составные). Назначение СУБД. Определение всех элементов СУБД и их характеристики. Переход от логической к физической. На примере MS SQL Server или другой аналогичной СУБД. Определение ключей, назначение, примеры.
23.СУБД. Определение, назначение, требования, основные компоненты. Назначения основных компонентов. Примеры СУБД. Определение, назначение, виды, примеры.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Критерии оценивания	Оценочные материалы	Критерии оценивания

1.	ОК-8 - способность к самоорганизации и самообразованию	***знать:*** - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; ***уметь:*** - самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;	Собеседование, Практическая работа с разделением на подгруппы	Компетенции сформированы при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-10 - способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	**Знать:** области применения систем управления базами данных; особенности управления данными в системах распределенной обработки; особенности управления данными в системах распределенной обработки; работы с системами управления базами данных на различных платформах; **Уметь:** разрабатывать программы на высокоуровневых языках программирования ;	Собеседование, Практическая работа с разделением на подгруппы	

		применять навыки разработчика и администратора баз данных		

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Шустова, Л. И. Базы данных : учебник / Л. И. Шустова, О. В. Тараканов. — Москва : ИНФРА-М, 2019. — 304 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-010485-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1009760 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

7.2. Дополнительная литература:

7. 1. Култыгин, О. П. Администрирование баз данных. СУБД MS SQL Server [Электронный ресурс] : учеб. пособие / О. П. Култыгин. - Москва : МФПА, 2012. - 232 с. - (Университетская серия). - ISBN 978-5-4257-0026-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/451114 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

8. 2. Мартишин, С. А. Базы данных: Работа с распределенными базами данных и файловыми системами на примере MongoDB и HDFS с использованием Node.js, Express.js, Apache Spark и Scala : учеб. пособие / С.А. Мартишин, В.Л. Симонов, М.В. Храпченко. — Москва : ИНФРА-М, 2019. — 235 с. + Доп. материалы [Электронный ресурс; URL: http://new.znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cc063e18baca3.52928692. - ISBN 978-5-16-015133-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1018196 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

7.3. Интернет-ресурсы

1. вузовские электронно-библиотечные системы учебной литературы.
2. база научно-технической информации ВИНИТИ РАН
3. доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru
4. sql-tutorial.ru.

7.4 Современные профессиональные базы данных и информационные справочные системы

Базы данных научно-технической информации, научных трудов, статей и других материалов, доступных в Тюменском государственном университете https://www.utmn.ru/upload/medialibrary/fc5/Perechen-podpisnykh-litsenzionnykh-baz-dannykh-i-baz-dannykh-dostupnykh-v-ramkakh-natsionalnoy-podpiski.doc (дата обращения: 15.05.2020).

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Среды разработки на языках C#, C++, Delphi;
- Системы управления базами данных: MS SQL Server, InterBase/FireBird, MySQL;
- Средство моделирования MS Office Visio
- Средство электронного обучения Microsoft Teams

9. **Технические средства и материально-техническое обеспечение дисциплины (модуля)**

Для организации самостоятельной работы студентов необходим компьютерный класс с пакетом прикладных программ, в том числе с установленной средой разработки на языке C#, C++, Pascal, Java, с системами управления базами данных: MS SQL Server, InterBase/FireBird, MySQL, со средством моделирования MS Office Visio.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020г.

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Атманских М.Б., Ниссенбаум О.В. Теоретико-числовые методы в криптографии. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Криптографические методы защиты информации [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Атманских М.Б., Ниссенбаум О. В. 2020.

1. Пояснительная записка

Теоретико-числовые методы в криптографии является дисциплиной обеспечивающей приобретение знаний по математическим основам криптографической защиты информации.

Целью дисциплины «Теоретико-числовые методы в криптографии» является изложение базовых принципов построения и математического обоснования криптографических систем.

Задачи курса - изучение:

- Теоретико-числовых, алгебраических, аналитических и вероятностных подходов к построению и анализу криптосистем;
- Математические основ криптографии;
- Математических методов, используемых в криптоанализе

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Информатика», «Структуры и алгоритмы компьютерной обработки информации», «История криптографии».

Дисциплина «Теоретико-числовые методы в криптографии» способствует освоению следующих дисциплин: «Криптографические протоколы», «Криптографические методы защиты информации».

1.2.**Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*) УП компетенции**

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОПК-2 – способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов		знать: - теоретико-числовые основы двухключевой криптографии; основы дискретной алгебры и теории чисел; алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; уметь: - проводить оценку сложности алгоритмов; выполнить постановку задач криптоанализа и указать подходы к их решению; использовать основные математические методы, применяемые в синтезе и анализе типовых криптографических алгоритмов.
ПК-5 – способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая		знать: - основные задачи и понятиях криптографии; основные виды асимметричных криптографических алгоритмов. уметь: - корректно применять симметричные и асимметричные

защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		криптографические алгоритмы; формализовать поставленную задачу.

* не предусмотрено

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		4 семестр
Общий объем зач. ед.	3	3
час.	108	108
Из них:		
Часы аудиторной работы (всего):	72	72
Лекции	36	36
Практические занятия	36	36
Лабораторные/практические занятия по подгруппам	0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	36	36
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной) и традиционной систем оценок.

Оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических работ на занятиях с разделением на подгруппы. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 100 баллов – зачтено.

Оценка «зачтено» ставится, если студент набрал 61 балл или выше. Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать зачет.

Оценка студента на зачете в рамках традиционной системы оценок выставляется на основе ответа студента на теоретические вопросы. Эта оценка характеризует уровень знаний, умений и навыков, приобретенных студентом в ходе изучения дисциплины.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса и практическое задание из пройденных тем на усмотрение преподавателя. Для получения оценки «зачтено»

студентом должно быть сдано минимум 5 практических работ на занятиях с разделением на подгруппы и сделан ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности.
Примечание. Студент, желающий исправить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу зачета.

4. Содержание дисциплины
4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Введение в математические проблемы криптографии. Основы теории чисел.	16	4	4	0	0
2.	Теория сравнений. Вычеты.	12	4	4	0	0
3.	Сравнения первой степени. Системы сравнений первой степени	16	6	6	0	0
4.	Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.	16	6	6	0	0
5.	Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа.	16	6	6	0	0
6.	Алгоритмы криптоанализа шифров с открытым ключом	16	6	6	0	0

7.	Конечные группы и поля многочленов	16	4	4	0	0
	Итого (часов)	108	36	0	36	0

4.2. Содержание дисциплины (*модуля*) по темам

Тема 1. Введение в математические проблемы криптографии. Основы теории чисел. Делимость, простые числа, наибольший общий делитель. Алгоритм Евклида, расширенный алгоритм Евклида. Цепные дроби. Асимптотический закон распределения простых чисел. Мультипликативные функции. Функция Эйлера.
Тема 2. Теория сравнений. Вычеты.
Полная система вычетов, приведенная система вычетов. Zn, Zp, Z*n, Z*p Обратный элемент в Zn Алгебраические структуры на целых числах. Теорема Эйлера, теорема Ферма, тест Ферма на простоту. Криптосистема RSA. Понижение степени сравнения.
Тема 3. Сравнения первой степени. Системы сравнений первой степени.
Сравнения первой степени и их решение. Системы сравнений первой степени и их решение. Китайская теорема об остатках и ее применения в криптографии (схема разделения секрета на ее основе и ее применение в RSA).
Тема 4. Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.
Квадратичные сравнения. Символ Лежандра. Закон взаимности. Существование решений квадратичного сравнения по простому модулю. Решение квадратичных сравнений по простому модулю. Символ Якоби и его свойства. Тест Соловея-Штрассена на простоту. Существование и количество решений квадратичного сравнения по составному модулю. Решение квадратичных сравнений по составному модулю. Квадраты и псевдоквадраты. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. Числа Блюма. BBS-генератор. Криптосистемы Блюма-Гольдвассер, Гольдвассер-Микали.
Тема 5. Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа.
Циклическая группа Z*p (Up). Порождающий элемент и дискретный логарифм. Задача дискретного логарифмирования. Криптосистемы Диффи-Хэллмана и Эль-Гамаля. Теоремы Сэлфриджа и Поклингтона. (n-1) – тесты на простоту. Доказуемо простые числа общего вида. Числа Ферма, теорема Пепина, тест Пепина. Числа Мерсенна и тест ЛукасаЛемера. Теорема Диемитко и процедура генерации простых чисел ГОСТ Р34.10-94.
Тема 6. Алгоритмы криптоанализа шифров с открытым ключом.
Элементы теории сложности. Оценки сложности по времени, по объему требуемой памяти. Полиномиальная сложность, субэкспоненциальная сложность, экспоненциальная сложность алгоритмов. Сложность элементарных операций. Теоретико-числовые проблемы, лежащие в основе двухключевых криптосистем – факторизация, дискретное логарифмирование. Алгоритмы факторизации. Метод пробных делений, метод Ферма, метод квадратичного решета, ро-метод Полларда, р—1 – метод Полларда, методы случайных квадратов. Примеры, оценки сложности указанных алгоритмов. Алгоритмы

дискретного логарифмирования. Метод прямого поиска, ро-метод Полларда, метод исчисления индексов, «шаг младенцашаг великана». Примеры, оценки сложности указанных алгоритмов.
Тема 7. Конечные группы и поля многочленов.
Многочлены над Zp, Zn. Сложение, умножение, факторизация многочленов. Неприводимые многочлены. Поля Галуа.

Планы практических занятий
Тема 1. Введение в математические проблемы криптографии. Основы теории чисел.
1. Операции над целыми числами. Нахождение наибольшего общего делителя при помощи алгоритма Евклида, наименьшего общего кратного. Построение таблицы первых простых чисел с помощью решета Эратосфена. Нахождение канонического разложения числа на простые сомножители.
Тема 2. Теория сравнений. Вычеты.
1. Разложение дробей в цепные дроби при помощи алгоритма Евклида. Асимптотический закон распределения простых чисел – вычисление примерного количества простых чисел на заданном интервале.
2. Вычисление функции Эйлера от числа. Теория сравнений. Построение приведенной системы вычетов от по заданному модулю. Проверка сравнений.
3. Вычисление обратного элемента в Zn при помощи расширенного алгоритма Евклида. Тест Ферма на простоту. Понижение степени сравнения при помощи теоремы Эйлера. Криптосистема RSA.
Тема 3. Сравнения первой степени. Системы сравнений первой степени
1. Сравнения первой степени и их решение.
2. Системы сравнений первой степени и их решение по Китайской теореме об остатках.
3. Контрольная работа.
Тема 4. Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту
1. Символ Лежандра. Существование решений квадратичного сравнения по простому модулю. Решение квадратичных сравнений по простому модулю.
2. Символ Якоби. Существование и количество решений квадратичного сравнения по составному модулю. Решение квадратичных сравнений по составному модулю.
3. Квадраты и псевдоквадраты. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. Числа Блюма. BBS-генератор. Криптосистемы Блюма-Гольдвассер, Гольдвассер-Микали. Циклическая группа Z*p (Up). Отыскание порождающего элемента. Контрольная работа.
Тема 5. Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа
1. (n-1) – тесты на простоту на основе теорем Сэлфриджа и Поклингтона.
2. Числа Ферма, тест Пепина. Числа Мерсенна и тест Лукаса-Лемера. Процедура генерации простых чисел ГОСТ Р34.10-94.
Тема 6. Алгоритмы криптоанализа шифров с открытым ключом.

1. Алгоритмы факторизации. Метод пробных делений, метод Ферма, метод квадратичного решета.
2. Ро-метод Полларда, р—1 – метод Полларда, методы случайных квадратов. Примеры, оценки сложности указанных алгоритмов.
3. Алгоритмы дискретного логарифмирования. Метод прямого поиска, «шаг младенца-шаг великана», ро-метод Полларда.
4. Метод исчисления индексов, метод Полига-Хэллмана. Примеры, оценки сложности указанных алгоритмов.
Тема 7. Конечные группы и поля многочленов.
1. Вычисления в конечных кольцах многочленов. Сумма, произведение многочленов, разложение многочлена на сомножители
2. Неприводимые многочлены, проверка многочлена на простоту. Нахождение обратного.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Введение в математические проблемы криптографии. Основы теории чисел.	Конспектирование материала на лекционных занятиях. Выполнение домашней контрольной работы. Работа с учебной литературой. Подготовка к коллоквиуму и контрольной работе
2.	Теория сравнений. Вычеты.	Конспектирование материала на лекционных занятиях. Выполнение домашней контрольной работы. Работа с учебной литературой. Подготовка к коллоквиуму и контрольной работе
3.	Сравнения первой степени. Системы сравнений первой степени.	Конспектирование материала на лекционных занятиях. Выполнение домашней контрольной работы. Работа с учебной литературой. Подготовка к коллоквиуму и контрольной работе
4.	Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.	Конспектирование материала на лекционных занятиях. Выполнение домашней контрольной работы. Работа с учебной литературой. Подготовка к коллоквиуму и контрольной работе
5.	Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа.	Конспектирование материала на лекционных занятиях. Выполнение домашней контрольной работы. Работа с учебной литературой. Подготовка к коллоквиуму и контрольной работе
6.	Алгоритмы криптоанализа шифров с открытым ключом.	Конспектирование материала на лекционных занятиях. Выполнение домашней контрольной работы. Работа с учебной литературой. Подготовка к коллоквиуму и контрольной работе
7.	Конечные группы и поля многочленов	Конспектирование материала на лекционных занятиях. Выполнение домашней контрольной работы. Работа с учебной литературой. Подготовка к коллоквиуму и контрольной работе

Порядок выполнения каждого вида самостоятельной работы:

Для подготовки к собеседованиям и коллоквиумам необходимо пользоваться конспектом лекций и [1] из списка основной литературы. Для выполнения расчетных работ на практических занятиях с разделением на подгруппы следует использовать [1] из дополнительной литературы, методички и раздаточный материал, выдаваемые преподавателем и хранящиеся на кафедре информационной безопасности. Для получения расширенных и углубленных знаний по тематике рекомендуется пользоваться ссылками из списка интернет-ресурсов, приведенных в данном УМК, а также электронными и бумажными номерами научных журналов, имеющихся в ИБЦ, областной научной библиотеке и сети интернет. Особенное внимание рекомендуется обратить на издания «Математические вопросы криптографии», «Прикладная дискретная математика», материалами конференций RealWorldCrypto, Crypto, Eurocrypt, Ruscrypt, Sibecrypt, Asiacrypt.

Контроль за самостоятельной работой осуществляется на коллоквиуме.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения зачета – комплект заданий для зачета

Вопросы к зачету

1. Основные понятия теории чисел. Теорема делимости.
2. Наибольший общий делитель и алгоритм Евклида.
3. Цепные дроби и алгоритм Евклида.
4. Наименьше общее кратное. Простые числа.
5. Теоремы Евклида о простых числах. Решето Эратосфена.
6. Основные свойства простых чисел. Теорема о единственности разложения на простые сомножители.
7. Теорема о делителях числа и ее следствия.
8. Асимптотический закон распределения простых чисел.
9. Функция Эйлера, ее свойства.
10. Сравнения. Свойства сравнений.
11. Полная система вычетов, приведенная система вычетов. Алгебраические свойства, обратный элемент.
12. Теорема Эйлера, теорема Ферма. Следствие.
13. Тест Ферма на простоту. Числа Кармайкла. Теорема Кармайкла.
14. Применение теоремы Ферма в криптосистеме RSA.
15. Сравнения с одним неизвестным 1-й степени.
16. Система сравнений 1-й степени. Китайская теорема об остатках.
17. Применение Китайской теоремы об остатках в RSA и схема разделения секрета на ее основе.
18. Квадратичные сравнения по простому модулю.
19. Символ Лежандра и его свойства.
20. Решение квадратичных сравнений по простому модулю.
21. Число решений квадратичного сравнения по составному модулю.
22. Символ Якоби, его свойства. Тест Соловея-Штрассена.

23. Квадратичные сравнения по модулю RSA. Связь задач извлечения корней и факторизации. Криптосистема Рабина.
24. Квадраты и псевдоквадраты. Числа Блюма.
25. BBS-генератор. Криптосистема Блюма-Гольдвассер, криптосистема ГольдвассерМикали.
26. Тест Миллера-Рабина.
27. Порядок группы. Порядок элемента в группе. Порождающий элемент.
28. Существование порождающего элемента в Z*n
29. Критерий Люка.
30. Теорема Сэлфриджа и тест Миллера.
31. Теорема Поклнгтона и тест на простоту на ее основе.
32. Числа Ферма, теорема Пепина, тест Пепина.
33. Числа Мерсена. Тест Лукаса-Лемера.
34. Теорема Диемитко. Процедура генерации простых чисел ГОСТ Р 34.10-94. 35. Дискретный логарифм. Проблема Диффи-Хелмана. Криптосистема ЭльГамаля.
36. Кольца многочленов.
37. Поле многочленов GF(pα).
38. Проблема факторизации. Метод пробных делений.
39. Метод Ферма факторизации.
40. Метод квадратичного решета.
41. Ро-метод Полларда факторизации.
42. p—1 – метод факторизации.
43. Методы случайных квадратов.
44. Задача дискретного логарифмирования. Метод прямого поиска.
45. Ро-метод Полларда дискретного логарифмирования.
46. Алгоритм Полига-Хеллмана.
47. Метод «Шаг младенца-шаг великана».
48. Метод исчисления порядка

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (из паспорта компетенций)*	Оценочные материалы	Критерии оценивания
1.	ОПК-2 – способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей,	знать: - теоретико-числовые основы двухключевой криптографии; основы дискретной алгебры и теории чисел; алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в	Контрольные работы, коллоквиум, задание для зачета	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п.

	математической статистики, теории информации, теоретико-числовых методов	конечных циклических группах.; уметь: - проводить оценку сложности алгоритмов; выполнить постановку задач криптоанализа и указать подходы к их решению; использовать основные математические методы, применяемые в синтезе и анализе типовых криптографических алгоритмов.		4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-5 – способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	знать: - основные задачи и понятиях криптографии; основные виды асимметричных криптографических алгоритмов. уметь: - корректно применять симметричные и асимметричные криптографические алгоритмы; формализовать поставленную задачу.	Контрольные работы, коллоквиум, задание для зачета	

* - не предусмотрен

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учеб. пособие / М.М. Глухов [и др.]. — Электрон. дан. — Санкт-Петербург : Лань, 2011. — 400 с. — Режим доступа: https://e.lanbook.com/book/68466. (дата обращения: 15.05.2020).

7.2. Дополнительная литература:

1. Виноградов, И.М. Основы теории чисел [Электронный ресурс] : учеб. пособие — Электрон. дан. — Санкт-Петербург: Лань, 2009. — 176 с. — Режим доступа: https://e.lanbook.com/book/46 (дата обращения: 15.05.2020).
2. Крамаров С.О. Криптографическая защита информации: учеб. пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — М.: РИОР: ИНФРА-М, 2018. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6 [Электронный ресурс]. - URL: http://znanium.com/catalog/product/901659 (дата обращения: 15.05.2020).

7.3. Интернет-ресурсы

- вузовские электронно-библиотечные системы учебной литературы.
- доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru
- A. Menezes, P. van Oorschort, S. Vanstone, Handbook of Applied Cryptography – CRC Press Inc., 5th Printing, 2001 [On-line] http://www.cacr.uwaterloo.ca/hac/
- http://www.ietf.org/rfc.html [On-line] - документы IETF – инженерного совета Интернета
- http://www.iacr.org/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- платформа для электронного обучения Microsoft Teams.
- Open Office Calc

9. **Технические средства и материально-техническое обеспечение дисциплины (модуля)**

- Учебные аудитории для проведения лекций и практических занятий;
- Лаборатории, оснащенные лабораторным оборудованием;
- Учебные аудитории для проведения занятий лекционного и семинарского типа, консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы. Для проведения занятий лекционного типа необходимо демонстрационное оборудование. Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Пряхин И.И. Техническая защита информации. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Техническая защита информации [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Пряхин И.И., 2020.

1. Пояснительная записка

Дисциплина «Техническая защита информации» является дисциплиной профессионального цикла ООП подготовки специалистов. Учитывая, что в ходе профессиональной деятельности специалисты этого направления будут иметь дело с информацией различного рода и различного уровня секретности, знание основных способов и средств съёма и защиты информации позволит им успешно решать профессиональные задачи. Дисциплина «Техническая защита информации» посвящена изучению основных каналов распространения информации и способов защиты информации в этих каналах от несанкционированного доступа.

Цель дисциплины «Техническая защита информации» - теоретическая и практическая подготовленность специалиста к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в защищаемых помещениях.

Задачи курса:

- ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- ознакомление с техническими каналами утечки акустической (речевой) информации;
- изучение способов и средств защиты информации, обрабатываемой техническими средствами;
- изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Математика», «Общая физика», «Криптографические методы защиты информации», «Основы информационной безопасности».

Дисциплина «Техническая защита информации» способствует освоению следующих дисциплин: «Администрирование и безопасность SQL Server».

1.2.**Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)**

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОПК-1 - способность анализировать физические явления и процессы при решении профессиональных задач		Знать: - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; - технические каналы утечки информации, возможности технических разведок, способы и

		средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; Уметь: -анализировать и оценивать угрозы информационной безопасности объекта;
ПК-12 - способность проводить инструментальный мониторинг защищенности компьютерных систем		Знать: - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; Уметь: - анализировать и оценивать угрозы информационной безопасности объекта; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
ПК-19 - способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации		Знать: - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; Уметь: - анализировать и оценивать угрозы информационной безопасности объекта;
ПК-9 - способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы		Знать: - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; - технические каналы утечки информации, возможности

		технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; Уметь: - анализировать и оценивать угрозы информационной безопасности объекта;

* не предусмотрено

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		8 семестр
Общий объем зач. ед.	4	4
час.	144	144
Из них:		
Часы аудиторной работы (всего):	72	72
Лекции	36	36
Практические занятия	0	0
Лабораторные/практические занятия по подгруппам	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	72	72
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		экзамен

3. Система оценивания

3.1. Для текущего контроля применяется 100-балльная система оценивания. Баллы проставляются за выполнение практических работ по каждой теме дисциплины. Результаты текущего контроля учитываются при промежуточной аттестации. Перевод баллов в оценки осуществляется по следующей шкале: от 91 до 100 баллов – «отлично»; от 76 до 90 баллов – «хорошо»; от 61 до 75 баллов – «удовлетворительно». Обучающиеся, не набравшие достаточного количества баллов для оценки, сдают экзамен в период экзаменационной сессии. Экзамен проводится в традиционной форме по билетам, содержащим 3 вопроса: 2 теоретических и 1 практический. В случае, если обучающийся в течение семестра выполнил и сдал менее 7 практических работ, экзаменатор имеет право задать ему дополнительные практические вопросы в количестве равном 7 минус количество сданных практических работ.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные/практические занятия по подгруппам	
1	2	3	4	5	6	7
1	Введение. Характеристика государственной системы противодействия технической разведке	4	2	0	0	0
2	Обнаружение и локализация источников радиоизлучений	4	0	0	2	0
3	Нормативные документы по противодействию технической разведке	4	2	0	0	0
4	Цифровые диктофоны	4	0	0	2	0
5	Демаскирующие признаки объектов наблюдения и сигналов	4	2	0	0	0
6	Генераторы радиошума и блокираторы источников радиосигналов	4	0	0	2	0
7	Средства и методы технической разведки	4	2	0	0	0
8	Обнаружение и локализация закладных устройств с помощью нелинейного локатора	4	0	0	2	0
9	Способы и средства перехвата сигналов. Способы	4	2	0	0	0

	и средства наблюдения					
10	Многофункциональные поисковые приборы, ST-031 «Пиранья»	4	0	0	2	0
11	Технические каналы утечки информации	4	2	0	0	0
12	Универсальный анализатор проводных линий «УЛАН-2»	4	0	0	2	0
13	Оптические и радиоэлектронные каналы утечки информации	4	2	0	0	0
14	Акустоэлектрические преобразователи	4	0	0	2	0
15	Акустические и виброакустические каналы утечки информации	4	2	0	0	
16	Многофункциональные поисковые приборы, ST-032	4	0	0	2	
17	Средства обнаружения технических каналов утечки информации	4	2	0	0	
18	Детектор электромагнитного поля ST 007	4	0	0	2	
19	Мероприятия по выявлению средств технической разведки	4	2	0	0	
20	Принципы дозиметрической разведки. Дозиметрия ионизирующих излучений	4	0	0	2	
21	Методы и средства защиты информации от утечки по техническим каналам	4	2	0	0	
22	Обнаружение и локализация	4	0	0	2	

	акустических закладных устройств, программный коррелятор «OSCOR»					
23	Скрытие речевой информации в каналах связи	4	2	0	0	
24	Измерение ПЭМИ монитора и оценка величины зоны R2	4	0	0	2	
25	Обнаружение и локализация закладных устройств	4	2	0	0	
26	Изучение устройства и работы лазерного микрофона	4	0	0	2	
27	Концепция и методы инженернотехнической защиты информации	4	2	0	0	
28	Генераторы акустического и виброакустического шума	4	0	0	2	
29	Виды контроля и расчёта эффективности защиты информации	8	4	0	0	
30	Дополнительная практическая работа	8	0	0	4	
31	Виды контроля и расчёта эффективности защиты информации	8	4	0	0	
32	Дополнительная практическая работа	8	0	0	4	
	Итого (часов)	144	36	0	36	2

4.2. Содержание дисциплины (*модуля*) по темам

Тема 1.1. Введение. Характеристика государственной системы противодействия технической разведке.

Нормативные документы по противодействию технической разведке.

Тема 1.2. Свойства и виды информации.

Виды, источники и носители защищаемой информации.

Тема 1.3. Демаскирующие признаки объектов наблюдения и сигналов.

Опасные сигналы и их источники.

Тема 1.4. История развития разведки и съема информации. Средства и методы технической разведки.

Классификация технической разведки, основные этапы и процедуры добывания информации технической разведкой.

Тема 1.5. Способы и средства перехвата сигналов.

Способы и средства наблюдения. Способы и средства подслушивания. Способы прослушивания помещений. Дистанционные системы прослушивания. Способы и средства добывания информации о радиоактивных веществах. Специальные системы получения информации.

Тема 2.1. Технические каналы утечки информации.

Характеристики технических каналов утечки информации, физические принципы технических каналов передачи информации.

Тема 2.2. Оптические и радиоэлектронные каналы утечки информации.

Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Электрические каналы утечки информации. Электромагнитные каналы утечки информации. Канал ПЭМИН. 10.

Тема 2.3. Акустические и виброакустические каналы утечки информации.

Материально-вещественные каналы утечки информации. Комплексное использование каналов утечки информации.

Тема 2.4. Средства обнаружения технических каналов утечки информации.

Средства обнаружения и локализации закладных устройств. Нелинейные локаторы. Сканирующие приёмники. Детекторы электромагнитного поля. Программно-аппаратные автоматизированные комплексы. Досмотровая техника.

Тема 2.5. Мероприятия по выявлению средств технической разведки.

Специальные проверки, специальные обследования, и специальные исследования.

Тема 3.1. Методы и средства защиты информации от утечки по техническим каналам. Пассивные и активные методы защиты.

Тема 3.2. Скрытие речевой информации в каналах связи.

Энергетическое скрытие акустических информативных сигналов.

Тема 3.3. Обнаружение и локализация закладных устройств, подавление их сигналов; подавление опасных сигналов акустоэлектрических преобразователей; экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания; подавление опасных сигналов.

Тема 3.4. Концепция и методы инженерно-технической защиты информации.

Методы и средства инженерной защиты и технической охраны объектов.

Тема 3.5. Виды контроля и расчёта эффективности защиты информации.

Физические принципы контроля защиты информации; основные положения методологии инженерно-технической защиты информации. Методы расчета и инструментального контроля показателей защиты информации. Средства измерения при инструментальном контроле.

Планы практических занятий

Семинарские занятия учебным планом не предусмотрены

Образцы средств для проведения текущего контроля

Текущий контроль – практическая работа – осуществляется в письменной форме в виде ответов на вопросы по пройденным темам.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ Темы	Темы	Виды СРС
1	2	3
1	Введение. Характеристика государственной системы противодействия технической разведке	Чтение обязательной и дополнительной литературы
2	Обнаружение и локализация источников радиоизлучений	Проработка лекций
3	Нормативные документы по противодействию технической разведке	Чтение обязательной и дополнительной литературы
4	Цифровые диктофоны	Проработка лекций
5	Демаскирующие признаки объектов наблюдения и сигналов	Чтение обязательной и дополнительной литературы
6	Генераторы радиошума и блокираторы источников радиосигналов	Проработка лекций
7	Средства и методы технической разведки	Чтение обязательной и дополнительной литературы
8	Обнаружение и локализация закладных устройств с помощью нелинейного локатора	Проработка лекций
9	Способы и средства перехвата сигналов. Способы и средства наблюдения	Чтение обязательной и дополнительной литературы
10	Многофункциональные поисковые приборы, ST-031 «Пиранья»	Проработка лекций

1	2	3
11	Технические каналы утечки информации	Чтение обязательной и дополнительной литературы
12	Универсальный анализатор проводных линий «УЛАН-2»	Проработка лекций
13	Оптические и радиоэлектронные каналы утечки информации	Чтение обязательной и дополнительной литературы
14	Акустоэлектрические преобразователи	Проработка лекций
15	Акустические и виброакустические каналы утечки информации	Чтение обязательной и дополнительной литературы
16	Многофункциональные поисковые приборы, ST-032	Проработка лекций
17	Средства обнаружения технических каналов утечки информации	Чтение обязательной и дополнительной литературы
18	Детектор электромагнитного поля ST 007	Проработка лекций
19	Мероприятия по выявлению средств технической разведки	Чтение обязательной и дополнительной литературы
20	Принципы дозиметрической разведки. Дозиметрия ионизирующих излучений	Проработка лекций
21	Методы и средства защиты информации от утечки по техническим каналам	Чтение обязательной и дополнительной литературы
22	Обнаружение и локализация акустических закладных устройств, программный коррелятор «OSCOR»	Проработка лекций
23	Скрытие речевой информации в каналах связи	Чтение обязательной и дополнительной литературы
24	Измерение ПЭМИ монитора и оценка величины зоны R2	Проработка лекций
25	Обнаружение и локализация закладных устройств	Чтение обязательной и дополнительной литературы
26	Изучение устройства и работы лазерного микрофона	Проработка лекций
27	Концепция и методы инженерно технической защиты информации	Чтение обязательной и дополнительной литературы
28	Генераторы акустического и виброакустического шума	Проработка лекций
29	Виды контроля и расчёта эффективности защиты информации	Чтение обязательной и дополнительной литературы
30	Дополнительная практическая работа	Проработка лекций
31	Виды контроля и расчёта эффективности защиты информации	Чтение обязательной и дополнительной литературы
32	Дополнительная практическая работа	Проработка лекций

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение рекомендованной основной и дополнительной литературы.
3. Разбор примеров практических работ.

Контроль за самостоятельной работой осуществляется при выполнении обучающимся теста, практической работы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Экзамен проводится в традиционной форме по билетам, содержащим 3 вопроса: 2 теоретических и 1 практический. В случае, если обучающийся в течение семестра выполнил и сдал менее 7 практических работ, экзаменатор имеет право задать ему дополнительные практические вопросы в количестве равном 7 минус количество сданных практических работ.

Экзамен выставляется автоматом в случае набора необходимого количества баллов:
от 61 до 75 – удовлетворительно;
от 76 до 90 – хорошо;
91 и более – отлично.

Примерный перечень вопросов к экзамену:

1. Основные защищаемые параметры информации и их смысл
2. Перечислите виды конфиденциальной информации и информации, относящейся к государственной тайне.
3. Классификация демаскирующих признаков(ДП) и их краткое описание
4. Видовые ДП (Примеры)
5. ДП сигналов(Примеры)
6. ДП веществ (Примеры)
7. Структурная схема наблюдения в оптическом диапазоне с пояснениями
8. Характеристики способов и средств наблюдения в оптическом диапазоне.
9. Характеристики и возможности зрительной системы человека.
10. Визуально-оптические приборы и их основные характеристики. Объективы для скрытного наблюдения
11. Приборы ночного видения и тепловизоры.
12. Принцип работы электронно-оптического преобразователя
13. Принцип работы ПЗС. 14. Виды досмотровой техники
15. Принцип работы и применение вихретоковых приборов
16. Принцип работы и применение нелинейных локаторов
17. Способы и средства наблюдения в радиодиапазоне.
18. Задачи, решаемые при перехвате сигналов и структура типового комплекса для перехвата.
19. Виды и характеристики антенн.
20. Радиоприёмники (сканеры) и их характеристики и применение.
21. Способы и средства прослушивания, возможности слуховой системы человека.
22. Виды микрофонов и их принцип действия
23. Направленные и лазерные микрофоны.
24. Стетоскопы и телефонные закладки.
25. Метод ВЧ-навязывания и его применение для добывания информации.
26. Физические АЭП - преобразователи – источники опасных сигналов.
27. Закладные устройства и их характеристики.
28. Характеристики закладных устройств, затрудняющие их обнаружение.

29. Средства и методы (не меньше двух) обнаружения закладных устройств.
30. Зоны НСД к телефонной линии(ТЛ) и способы подключения.
31. Способы и средства защиты ТЛ
32. Конфиденциальное совещание: несанкционированный съём информации и методы защиты от него.
33. Методы и средства защиты речевой информации.
34. Классификация и общий принцип применения индикаторов поля.
35. Беззаходовые методы прослушивания помещений по ТЛ.
36. Мобильные системы связи и их использование в информационных атаках. Способы защиты.
37. Использование для съёма информации и подавление диктофонов.
38. Классификация и характеристики технических каналов утечки информации.
39. Оптические каналы утечки информации (атака и защита).
40. Радиоэлектронные каналы утечки информации.
41. Пассивные и активные методы защиты информации в радиоэлектронном канале.
42. Акустические каналы утечки информации (атака и защита).
43. Пассивные и активные методы защиты информации в акустическом канале.
44. Материально-вещественные каналы утечки информации.
45. Способы и принципы инженерно-технической защиты информации.
46. Способы и средства инженерной защиты и технической охраны объектов.
47. Классификация каналов ПЭМИН и утечка информации.
48. Пассивные и активные способы защиты в канале ПЭМИ.
49. Пассивные и активные способы защиты от наводок и просачиваний сигналов в линии заземления и питания.
50. Зоны электромагнитного поля и возможности утечки информации.
51. Контролируемая зона и критерий защищённости СВТ.
52. Определение зон R2, R1.
53. Анализатор проводных линий «Улан 2». Чистая линия.
54. Анализатор проводных линий «Улан 2». Обесточенная линия с подключением.
55. Многофункциональный прибор ST031. Поиск в эфире и в линии.
56. Многофункциональный прибор ST031. Поиск, измерение частоты.
57. Многофункциональный прибор ST031. Работа в канале АВАК.
58. Применение прибора «Сириус». Амплитудный метод поиска.
59. Применение прибора «PROTECT 1203». Настройка порогового устройства.
60. Применение прибора «ST007». Поиск.
61. Применение прибора «ST007». Измерение частоты.
62. Параметры и применение прибора «Баррикада»
63. Параметры и применение прибора «ГШ 1000»
64. Применение дозиметра. Фоновое излучение. Дозы излучения

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/ функциональный)	Оценочные материалы	Критерии оценивания
1.	ОПК-1 - способность анализировать физические явления и процессы при решении	Знать: - основные нормативные правовые акты в области информационной безопасности и защиты	Практические работы. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при

	профессиональных задач	информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; Уметь: -анализировать и оценивать угрозы информационной безопасности объекта;		глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-12 - способность проводить инструментальный мониторинг защищенности компьютерных систем	Знать: - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; Уметь: - анализировать и оценивать угрозы информационной безопасности объекта; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;	Практические работы. Экзамен.	

3.	ПК-19 - способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации	Знать: - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; Уметь: - анализировать и оценивать угрозы информационной безопасности объекта;	Практические работы. Экзамен.	
4.	ПК-9 - способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	Знать: - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; Уметь: - анализировать и оценивать угрозы информационной безопасности объекта;	Практические работы. Экзамен.	

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

4. 1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

7.2. Дополнительная литература:

1. Креопалов, В. В. Технические средства и методы защиты информации : учебное пособие / В. В. Креопалов. — Москва : Евразийский открытый институт, 2011. — 278 c. — ISBN 978-5-374-00507-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/10871.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. Пользователей
2. Мельников, В. П. Информационная безопасность и защита информации: учеб. пособие для студ. высш. проф. образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков. — 6-е изд., стер. — Москва: Академия, 2012 — 336 с. — (Высшее профессиональное образование). — Доступ по паролю из сети Интернет (чтение). — URL:https://library.utmn.ru/dl/IDO/978-5-7695-9222-5.pdf. - (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

7.3. Интернет-ресурсы

1. http://www.fstec.ru
2. http://www.smersh.ru
3. http://window.edu.ru/window/library?p_rid=63611

7.4. Современные профессиональные базы данных и информационные справочные системы

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

1. Пакет офисного программного обеспечения Microsoft Office или аналог.
2. elearning.utmn.ru
3. Платформа для электронного обучения Microsoft Teams.
4. Интернет, доступ в информационно-образовательную среду ТюмГУ, включающую в себя доступ к учебным планам и рабочим программам, к изданиям электронной библиотечной системы и электронным образовательным ресурсам.

9. **Технические средства и материально-техническое обеспечение дисциплины (модуля)**

Лекционные аудитории с мультимедийным оборудованием, компьютерные классы и специально оборудованные аудитории для проведения практических работ.

Практикум проводится в лаборатории технической защиты информации.

В лабораторном практикуме в том числе используются сертифицированные приборы, входящие в государственный реестр и предназначенные для проведения мероприятий по защите информации.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020г.

ТЕХНОЛОГИИ И МЕТОДЫ ПРОГРАММИРОВАНИЯ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Широких А.В. Технологии и методы программирования. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Технологии и методы программирования [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Широких А.В., 2020.

1. Пояснительная записка

Учебная дисциплина «Технологии и методы программирования» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Технологии и методы программирования» является изложение основополагающих принципов разработки программного обеспечения в различных средах с использованием различных информационных технологий при решении разнообразных прикладных задач.

Задачи дисциплины «Технологии и методы программирования»

- дать представление о компьютерных технологиях и методах программирования;
- научить использовать компьютерные технологии и методы программирования для решения разнообразных прикладных задач.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Математическая логика и теория алгоритмов», «Структуры и алгоритмы компьютерной обработки данных», «Языки программирования», «Дискретная математика».

Дисциплина «Технологии и методы программирования» способствует освоению следующих дисциплин: «Защита операционных систем», «Криптографические протоколы».

1.2. **Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)**

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОПК-8 - способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач		Знает: аспекты использования информационных технологий в различных языках и системах программирования для решения профессиональных, исследовательских и прикладных задач; Умеет: применять информационные технологии в различных языках и системах программирования для решения профессиональных, исследовательских и прикладных задач
ОПК-10 - способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах		Знает: основные методы описания, и анализа алгоритмов; Умеет: формулировать, разрабатывать и проводить реализацию алгоритмов

* не предусмотрено

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	Всего часов (академические часы)	Часов в семестре (академические часы)	
		5 семестр	**6** семестр
Общий объем зач. ед.	**7**	**4**	**3**
час.	**252**	**144**	**108**
Из них:			
Часы аудиторной работы (всего):	**144**	**72**	**72**
Лекции	72	36	36
Практические занятия			
Лабораторные/практические занятия по подгруппам	72	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	**108**	**72**	**36**
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет	экзамен

3. Система оценивания

3.1.

Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной) и традиционной (5-балльной) систем оценок.

В 5 семестре предусмотрен зачет. Оценка за зачет студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических работ, индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины. Для получения зачета необходимо набрать не менее 61 балла.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «зачет» студент должен сдать минимум 75% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы, и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты.

В 6 семестре предусмотрен экзамен. Экзаменационная оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических работ, индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должно быть сдано минимум 50% практических работ и сделан ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен сдать минимум 75% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен сдать минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами.

Примечание. Студент, желающих исправить экзаменационную оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
Семестр 5						
1	Введение в дисциплину	13	2		2	
2	Разработка с использованием скриптовых языков программирования.	13	2		2	
3	Разработка Win32 приложений и библиотек	17	4		4	
4	Разработка консольных приложений	17	4		4	
5	Разработка оконных приложений	17	4		4	
6	Параллельное программирование	17	4		4	
7	Разработка и использование COM объектов	25	8		8	

8	Разработка и использование ActiveX объектов	25	8		8	
	Всего (часов) за семестр 5	144	36		36	
Семестр 6						
1	Разработка сетевых приложений	14	4		4	
2	Разработка сервисных приложений	10	2		2	
3	Разработка .NET-приложений	18	6		6	
4	Разработка внешних хранимых процедур для серверов баз данных	18	6		6	
5	VBA приложения	22	8		8	
6	Web приложения	26	10		10	
	Всего (часов) за семестр 6	108	36		36	2
	Итого (часов)	252	72		72	2

4.2. Содержание дисциплины (*модуля*) по темам

Семестр 5

Введение в дисциплину

Основные понятия. Виды программного обеспечения. Среды разработки. Обзор современных компьютерных технологий.

Практическая работа

Разработка и реализация рекурсивного алгоритма

Практическая работа

Разработка и реализация не рекурсивного алгоритма

Разработка с использованием скриптовых языков программирования.

Windows Scripting Host. Разработка на VBScript и JScript. Введение в VBA.

Практическая работа

Разработка простого приложения на языках VBScript, Jscript и VBA.

Разработка Win32 приложений и библиотек

Разработка Win32 приложений и библиотек. Динамические библиотеки. Соглашение о вызове. Использование динамических библиотек. Использование WinAPI. Проецируемая память.

Практическая работа

Разработка приложения, связывающегося с динамической библиотекой во время загрузки.

Практическая работа

Разработка приложения, связывающегося с динамической библиотекой во время выполнения.

Практическая работа

Разработка простой динамической библиотеки.

Практическая работа

Разработка библиотеки, связывающейся с программой.

Практическая работа

Разработка программ, взаимодействующих через файловую проекцию.

Разработка консольных приложений

Практическая работа

Разработка консольного приложения, обрабатывающего консольный ввод.

Практическая работа

Разработка консольного приложения, выдающего информацию с использованием экранных буферов.

Разработка оконных приложений

Разработка оконных приложений с использованием низкоуровневого и высокоуровневого API.

Практическая работа

Разработка GUI приложения на Delphi.

Практическая работа

Разработка GUI приложения на C++

Практическая работа

Разработка WPF приложения.

Практическая работа

Разработка приложения Windows Forms.

Параллельное программирование

Процессы, потоки и задачи. Проблемы параллельного выполнения. Средства синхронизации.

Практическая работа

Разработка программ взаимодействующих через файловую проекцию.

Разработка и использование COM объектов

Разработка и использование COM объектов COM-технологии. COM архитектура Windows. Интерфейсы. Структура реестра. Создание COM объектов. Разработка собственных COM-объектов. Отладка.

Практическая работа

Разработка COM клиента.

Практическая работа

Разработка COM клиента.

Разработка и использование ActiveX объектов

ActiveX подсистема. Разработка ActiveX клиентов. Разработка ActiveX серверов. Отладка. Использование объекта MSScriptControl.ScriptControl. Использование WMI объектов.

Практическая работа

Использование системных ActiveX серверов

Практическая работа

Использование системных ActiveX серверов

Практическая работа

Использование системных ActiveX серверов

Практическая работа

Разработка ActiveX клиента.

Практическая работа

Разработка ActiveX сервера.

Практическая работа

Разработка приложения с использованием объекта MSScriptControl.ScriptControl.

Семестр 6

Разработка сетевых приложений

TCP/IP. Именованные каналы.

Практическая работа

Разработка TCP клиента и сервера.

Практическая работа

Разработка UDP клиента и сервера.

Практическая работа

Разработка приложения, использующего именованные каналы.

Разработка сервисных приложений

Сервисные приложения. Особенности разработки и отладки сервисных приложений.

Практическая работа

Разработка сетевого приложения службы и ее клиентов.

Разработка .NET-приложений

Архитектура .NET. Отличия .NET от Win32.

Сборки и приложения. Разработка и регистрация сборок. Управляемый и неуправляемый код. Сериализация и десериализация. Маршалинг данных. Домены приложений.

Практическая работа

Разработка .NET приложения с использованием неуправляемого кода.

Практическая работа

Стандартная сериализация и десериализация.

Практическая работа

Пользовательская сериализация и десериализация.

Разработка внешних хранимых процедур для серверов баз данных

Разработка хранимых процедур для Microsoft SQL сервера, сервера Oracle и других серверов.

Практическая работа

Разработка внешних функций для СУБД Firebird.

Практическая работа

Разработка хранимых процедур для MS SQL сервера.

VBA приложения

VBA. Объектная модель. Разработка и отладка VBA приложений.

Практическая работа

Разработка простого VBA приложения

Практическая работа

Разработка простого VBA приложения

Практическая работа

Разработка VBA приложения с использованием форм

Практическая работа

Разработка VBA приложения с классами

Практическая работа

Разработка VBA приложения с классами

Практическая работа

Разработка VBA приложения использующего события

Web приложения

Виды web приложений. Web службы. Современные средства и технологии разработки web приложений.

Практическая работа

Разработка простого web приложения на PHP

Практическая работа

Разработка простого web приложения на ASP.NET Web Forms

Практическая работа

Разработка простого web приложения на ASP.NET MVC

Практическая работа

Разработка web службы и ее клиента

Практическая работа

Использовании `HttpListener`

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
Семестр 5		
1	Введение в дисциплину	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
2	Разработка с использованием скриптовых языков программирования.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
3	Разработка Win32 приложений и библиотек	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
4	Разработка консольных приложений	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
5	Разработка оконных приложений	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
6	Параллельное программирование	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
7	Разработка и использование COM объектов	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
8	Разработка и использование ActiveX объектов	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
Семестр 6		
1	Разработка сетевых приложений	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
2	Разработка сервисных приложений	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

3	Разработка .NET-приложений	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
4	Разработка внешних хранимых процедур для серверов баз данных	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
5	VBA приложения	Чтение обязательной и дополнительной литературы, подготовка к практическим работам
6	Web приложения	Чтение обязательной и дополнительной литературы, подготовка к практическим работам

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение основной и дополнительной литературы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации – зачет (5 семестр), экзамен (6 семестр). Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса.

Вопросы к зачету

5 семестр

1. Стек. Передача параметров. Возврат результата. Соглашения о вызове.
2. Динамически загружаемые библиотеки. Назначение. Загрузка библиотеки в разных средах: WIN32, .NET, Python. Использование функций библиотеки. Использование библиотекой функций приложения.
3. Разработка собственных динамических библиотек. Экспорт функций по имени и индексу. Кодирование (декорация) имен функций. Импорт и экспорт с использованием DEF файлов.
4. Низкоуровневая работа с консолью Windows: основные функции, объекты, буферы экрана, ввод и вывод информации. Примеры.
5. Проецируемая память: функции, объекты, использование в разных средах. Примеры
6. Средства синхронизации: критические секции, мьютексы, семафоры, события. Функции ожидания. Interlocked функции.
7. Потоки. Использование потоков в различных средах: .NET и Win32
8. COM и ActiveX технологии
9. Архитектура COM и ActiveX.
10. Раннее и позднее связывание
11. Идентификаторы интерфейсов и классов. Библиотеки типов. Интерфейсы и объекты.
12. Разработка COM клиентов в разных средах - .NET, C++, Delphi. Особенности.
13. Разработка ActiveX клиентов в разных средах - .NET, C++, Delphi, сценарии WSH, Python. Особенности.
14. Разработка COM серверов в разных средах - .NET, C++, Delphi. Особенности.
15. Разработка ActiveX серверов в разных средах - .NET, C++, Delphi, WSC. Особенности.
16. Упрощенная автоматизация в Delphi: предоставление объектов Delphi как объектов автоматизации используя объект TObjectDispatch. Примеры использования на примере MSScriptControl.ScriptControl.

17. Чтение и запись XML документов используя MSXML2.DOMDocument. Язык запросов XPath. Примеры.
18. Использование COM и ActiveX ADODB объектов для доступа к базам данных. Примеры.
19. Использование ActiveX объектов через интерфейс IDispatch. Примеры.
20. Автоматизация приложений Microsoft Office. Понятие объектной модели. Примеры автоматизации приложений Microsoft Office.
21. Языки разработки JS, VBS. Примеры работы с WMI объектами.
22. Разработка VBA приложений. Подключение библиотек типов и COM. Примеры

Вопросы к экзамену

6 семестр

1. Разработка сетевых приложений с использованием протокола TCP. Особенности. Примеры
2. Разработка сетевых приложений с использованием протокола UDP. Особенности. Примеры
3. Взаимодействие приложений с использованием именованных каналов. Особенности. Примеры
4. Приложения службы. Особенности. Примеры
5. Сборки и приложения. Разработка и регистрация сборок. Примеры.
6. Управляемый и неуправляемый код. Native методы. Обращение к native методам из управляемого кода. Примеры.
7. Сериализация и десериализация. Примеры.
8. Маршалинг данных. Примеры.
9. Домены приложений. Примеры.
10. Разработка хранимых процедур для Microsoft SQL сервера, сервера Oracle и других серверов. Особенности. Примеры.
11. Язык программирования VBA. Объектная модель приложения. Особенности. Примеры.
12. VBA: Функции, процедуры и классы. Настроки модулей. Другие объекты. Особенности. Примеры.
13. VBA: Элементы управления VBA в документах Microsoft Office. Особенности. Примеры.
14. VBA: Работа с экранными формами. Особенности. Примеры.
15. VBA: Обработка событий. Особенности. Примеры.
16. Web приложения. Основные разновидности. Примеры.
17. Web службы. WSDL. Разработка веб служб и ее клиентов в Visual Studio. Примеры.
18. Разработка простого web приложения на PHP. Особенности. Примеры.
19. Разработка простого web приложения на ASP.NET Web Forms. Особенности. Примеры.
20. Разработка простого web приложения на ASP.NET MVC. Особенности. Примеры.
21. Использовании HttpListener. Примеры.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания

1	ОПК-8 - способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Знает: основные языки и системы программирования, среды разработки и компьютерные технологии; Умеет: применять основные языки и системы программирования, среды разработки и компьютерные технологии в профессиональной деятельности	Практическая работа. Зачет. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 "Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ"
2	ОПК-10 - способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Знает: способы построения, анализа и реализации алгоритмов; Умеет: проводить построение, анализ и реализацию алгоритмов в современных программных комплексах	Практическая работа. Зачет. Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29

				"Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ"

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Затонский, А. В. Информационные технологии: разработка информационных моделей и систем : учебное пособие / А. В. Затонский. - Москва : РИОР : ИНФРА-М, 2020. - 344 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-369-01183-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1043096 (дата обращения: 15.05.2020).

7.2. Дополнительная литература:

1. Гуриков, С. Р. Введение в программирование на языке Visual Basic for Applications (VBA) : учебное пособие / С.Р. Гуриков. — Москва : ИНФРА-М, 2020. — 317 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/949045. - ISBN 978-5-16-013667-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/949045 (дата обращения: 02.02.2021). – Режим доступа: по подписке.
2. Гуриков, С. Р. Введение в программирование на языке Visual Basic for Applications (VBA) : учебное пособие / С.Р. Гуриков. — Москва : ИНФРА-М, 2020. — 317 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/949045. - ISBN 978-5-16-013667-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/949045 (дата обращения: 02.02.2021). – Режим доступа: по подписке.
3. Абрамян, М. Э. Практикум по программированию на языке Паскаль: массивы, строки, файлы, рекурсия, линейные динамические структуры, бинарные деревья : учеб. пособие / М. Э. Абрамян. - Ростов н/Д : Издательство ЮФУ, 2010. - 276 с. - ISBN 978-5-9275-0801-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/549917 (дата обращения: 02.02.2021). – Режим доступа: по подписке.

7.3. Интернет-ресурсы

1. вузовские электронно-библиотечные системы учебной литературы.
2. доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru.
3. https://microsofr.com/
4. https://embarcadero.com/
5. https://www.rsdn.ru/

7.4 Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) https://icdlib.nspu.ru/
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА https://rusneb.ru/
- Справочная правовая система КонсультантПлюс http://www.consultant.ru/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Онлайн библиотеки
- Облачные системы хранения: Google Drive, Yandex Disk и т.д.
- Облачные системы сбора и хранения информации: Документы Google, Google Формы;
- Системы публикации и распространения информации: Blogger.com и другие
- Системы онлайн конференций: Microsoft Teams
- Система онлайн тестирования: https://etest.mwlabs.ru
- Мессенджеры: Telegram, Viber

9. **Технические средства и материально-техническое обеспечение дисциплины (модуля)**

Лекционная аудитория с проектором. Компьютерный класс с установленным ПО. Как в лекционной аудитории, так и в компьютерном классе необходимо наличие разрешений на системные папки IIS, конфигурацию IIS, регистрацию COM объектов и библиотек типов, установке служб, сетевой доступ. При проведении лекций и выполнении практических работ используется следующее программное обеспечение: Delphi 7 или выше, Microsoft Visual Studio 19 или выше, IIS 7.0 или выше, Microsoft Office 2013 или выше, Python, PHP, Операционная система Windows 7 или более поздние версии, операционная система Linux (возможно WSL) с установленным компилятором gcc, MySql сервером и возможностью добавления пакетов, платформа для электронного обучения Microsoft Teams. Microsoft SQL Server, MySQL Server, NotePad++, FarManager.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

ЭЛЕКТРОНИКА И СХЕМОТЕХНИКА
Рабочая программа
для обучающихся по специальности
10.05.01 Компьютерная безопасность
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Монтанари С.Г. Электроника и схемотехника. Рабочая программа для обучающихся по специальности 10.05.01 Компьютерная безопасность, специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Электроника и схемотехника [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Монтанари С.Г.,2020.

1. Пояснительная записка

Целью дисциплины «Электроника и схемотехника» является изучение основ электроники, элементов теории сигналов и схемотехники преобразовательных, усилительных и генераторных элементов в информационных системах, системах автоматизации.

Задачами дисциплины являются:

− ознакомление студентов с основами преобразования электрических сигналов в линейных и нелинейных аналоговых и цифровых цепях;

− ознакомление с элементной базой электротехнических и электронных цепей;

− ознакомление с основными принципами преобразования электромагнитной энергии в устройствах усиления, выпрямления и генерации;

− ознакомление со схемотехникой аналоговых и цифровых устройств;

− получение практических навыков исследования радиоэлектронных устройств.

1.1. Место дисциплины в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины базовой части. Для освоения данной дисциплины необходимы знания и умения, приобретённые обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Физика», «Математический анализ».

Дисциплина «Электроника и схемотехника» способствует освоению следующих дисциплин: «Техническая защита информации»

1.2. **Компетенции обучающегося, формируемые в результате освоения данной дисциплины**

Код и наименование компетенции	Компонент (знаниевый/функциональный)
ОК-8: способность к самоорганизации и самообразованию	**Знать:** содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; **Уметь:** самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;
ПК-5: способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	**Знать:** основные принципы работы и проектирования электронных систем; особенности применения аналоговых и цифровых радиоэлектронных устройств. **Уметь:** рассчитывать простые аналоговые и цифровые радиоэлектронные устройства.
ПК-11: способность участвовать в проведении экспериментально-	**Знать:**

исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	основные параметры и принципы работы базовых аналоговых и цифровых функциональных элементов электроники. **Уметь:** оценивать степень достоверности результатов, полученных с помощью экспериментальных и теоретических методов исследований.
ПК-12: способность проводить инструментальный мониторинг защищенности компьютерных систем	**Знать:** основные физические понятия и принципы функционирования базовых электронных полупроводниковых компонентов в аналоговых и цифровых системах. **Уметь:** проводить базовые теоретические и экспериментальные исследования электронного оборудования и систем; оценивать степень достоверности результатов, полученных с помощью экспериментальных и теоретических методов исследований.
ПК-19: способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации	**Знать:** терминологию и символику, используемую в электронике, методы составления и чтения основных видов электрических схем; особенности применения аналоговых и цифровых радиоэлектронных устройств. **Уметь:** проводить базовые теоретические и экспериментальные исследования электронного оборудования и систем; проводить контрольные проверки работоспособности применяемых средств защиты информации.

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		7 семестр
Общий объем зач. ед.	**4**	**4**
час.	**144**	**144**
Из них:		
Часы аудиторной работы (всего):	**72**	**72**
Лекции	36	36
Практические занятия	0	0
Лабораторные/практические занятия по подгруппам	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	**72**	**72**
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		экзамен

3. Система оценивания

В течение семестра каждому студенту необходимо обязательно выполнить и защитить 6 лабораторных работ.

При текущем контроле учитывается несколько видов деятельности обучающихся:

- допуски к выполнению лабораторных работ (0 – 1 балла);
- выполнение лабораторной работы (0-2 баллов);
- подготовка и сдача отчета по лабораторной работе (0-3 баллов);
- защита лабораторной работы (0-7 баллов).

Особенность выполнения студентами лабораторных работ практикума заключается в предварительной самостоятельной теоретической подготовке по теме исследования. При подготовке от студентов потребуются умения и навыки работы с литературой и другими источниками информации. Кроме того, студенты должны изучить элементарные основы теории вероятности и математической статистики и применять их для обработки экспериментальных результатов.

Студенту рекомендуется следующая схема подготовки к лабораторному занятию:

- проработка конспекта лекций дисциплины «Электроника и схемотехника» по тематике лабораторной работы;
- чтение рекомендованной основной и дополнительной литературы по тематике лабораторной работы;
- заполнение лабораторного журнала и подготовка к допуску для выполнения работы;
- выполнение всех расчетов необходимых величин и погрешностей к ним в лабораторном журнале;
- подготовка отчета по лабораторной работе.

Обязательным условием освоения дисциплины является выполнение и защита всех лабораторных работ.

В семестре обучающийся выполняет и сдаёт все 6 лабораторных работы, и сдаёт экзамен в устной форме.

Экзаменационный билет содержит 2 теоретических вопроса по тематике лекционных занятий.

Ответы на экзаменационный билет оцениваются по следующим критериям:

"отлично" - студент дал полный ответ на теоретические вопросы;

"хорошо" - студент показал систематические знания по дисциплине, но имеются недочеты в ответах;

"удовлетворительно" - студент имеет представления об основных явлениях и законах, однако недостаточно владеет теоретическим материалом, и допускает в ответах ошибки, которые может исправить под руководством преподавателя;

"неудовлетворительно" - студент не имеет систематических знаний, слабо разбирается в теоретических вопросах, допускает принципиальные ошибки в ответах.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины, час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
Лекционные занятия						
1.	Полупроводниковые приборы.	8	4	0	0	0
2.	Биполярные транзисторы.	8	4	0	0	0
3.	Усилители электрических сигналов.	8	4	0	0	0
4.	Дифференциальный каскад.	12	6	0	0	0
5.	Генераторы электрических колебаний.	8	4	0	0	0
6.	Элементы цифровой электроники.	12	6	0	0	0
7.	Сигналы и их классификация.	8	4	0	0	0
8.	Прохождение гармонического сигнала через нелинейную цепь.	8	4	0	0	0
Лабораторные занятия						
9.	Исследование диодов.	12	0	0	6	0
10.	Исследование биполярного транзистора.	12	0	0	6	0
11.	Исследование инвертирующего и неинвертирующего усилителя на операционном усилителе.	12	0	0	6	0
12.	Исследование логических элементов цифровых интегральных микросхем.	12	0	0	6	0
13.	Исследование JK-триггера и счетчика.	12	0	0	6	0
14.	Исследование параметрического стабилизатора напряжения.	12	0	0	6	0
	Итого (часов)	144	36	0	36	2*

* – учитывает контактную работу на консультации и экзамен.

4.2. Содержание дисциплины по темам

Темы лекционных занятий:

Тема 1. Полупроводниковые приборы. Электрические переходы и их свойства: *p-n* переход, переход металл-полупроводник. Диоды и их разновидности.

Тема 2. Биполярные транзисторы. Модель биполярного транзистора. Основные схемы включения. *h*-параметры. Полевые транзисторы, их разновидности и основные параметры.

Тема 3. Усилители электрических сигналов. Классификация усилителей, основные параметры. Элементы теории обратной связи в усилительных каскадах. Выбор рабочей точки. Усилительные каскады на биполярных и полевых транзисторах.

Тема 4. Дифференциальный каскад. Операционные усилители (ОУ). Классификация и основные параметры ОУ. Методы расчёта усилителей на ОУ. Применения ОУ.

Тема 5. Генераторы электрических колебаний. Классификация. *LC*- и *RC*-генераторы. Баланс амплитуд и фаз, мягкий и жесткий режим самовозбуждения. Стабилизация частоты.

Тема 6. Элементы цифровой электроники. Транзисторные ключи. Базовые логические элементы. Сумматоры. Триггеры, регистры, счетчики. Мультиплексоры и демультиплексоры. Шифраторы и дешифраторы. Аналого-цифровые и цифро-аналоговые преобразователи.

Тема 7. Сигналы и их классификация. Частотные и переходные характеристики простейших *RC*-цепей. Спектры периодических и непериодических сигналов. Преобразования Фурье и Лапласа. Случайные сигналы. Шумы в электронных устройствах.

Тема 8. Прохождение гармонического сигнала через нелинейную цепь. Модуляция и детектирование. Спектры сигналов с амплитудной, частотной и фазовой модуляцией. Амплитудный и частотный детектор. Синхронный детектор.

Темы лабораторных занятий:

Лабораторная работа №1. Исследование диодов.
Лабораторная работа №2. Исследование биполярного транзистора.
Лабораторная работа №3. Исследование инвертирующего и неинвертирующего усилителя на операционном усилителе.
Лабораторная работа №4. Исследование логических элементов цифровых интегральных микросхем.
Лабораторная работа №5. Исследование JK-триггера и счетчика.
Лабораторная работа №6. Исследование параметрического стабилизатора напряжения.

Все лабораторные работы по дисциплине проводятся в «Лаборатории радиоэлектроники и электротехники» ФТИ.

К каждой лабораторной работе имеются подробные методические рекомендации с необходимыми теоретическими сведениями, описанием установки, описанием последовательности выполнения заданий и обработки полученных результатов, а также список литературы.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
Лекционные занятия		
1.	Полупроводниковые приборы.	Проработка лекций. Работа с учебной литературой.
2.	Биполярные транзисторы.	Проработка лекций. Работа с учебной литературой.
3.	Усилители электрических сигналов.	Проработка лекций. Работа с учебной литературой.
4.	Дифференциальный каскад.	Проработка лекций. Работа с учебной литературой.
5.	Генераторы электрических колебаний.	Проработка лекций. Работа с учебной литературой.
6.	Элементы цифровой электроники.	Проработка лекций. Работа с учебной литературой.
7.	Сигналы и их классификация.	Проработка лекций. Работа с учебной литературой.
8.	Прохождение гармонического сигнала через нелинейную цепь.	Проработка лекций. Работа с учебной литературой.
Лабораторные занятия		
9.	Исследование диодов.	Проработка лекций. Подготовка к получению допуска и выполнению работы. Подготовка лабораторных журналов(необходимо для выполнения лабораторной работы).
10.	Исследование биполярного транзистора.	Проработка лекций. Подготовка к получению допуска и выполнению работы. Подготовка лабораторных журналов(необходимо для выполнения лабораторной работы).
11.	Исследование инвертирующего и неинвертирующего усилителя на операционном усилителе.	Проработка лекций. Подготовка к получению допуска и выполнению работы. Подготовка лабораторных журналов(необходимо для выполнения лабораторной работы).
12.	Исследование логических элементов цифровых интегральных микросхем.	Проработка лекций. Подготовка к получению допуска и выполнению работы. Подготовка лабораторных журналов(необходимо для выполнения лабораторной работы).
13.	Исследование JK-триггера и счетчика.	Проработка лекций. Подготовка к получению допуска и выполнению работы. Подготовка лабораторных журналов(необходимо для выполнения лабораторной работы).

14.	Исследование параметрического стабилизатора напряжения.	Проработка лекций. Подготовка к получению допуска и выполнению работы. Подготовка лабораторных журналов(необходимо для выполнения лабораторной работы).

Контроль за самостоятельной работой осуществляется при выполнении обучающимся лабораторных работ.

6. Промежуточная аттестация по дисциплине

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

Форма промежуточной аттестации – экзамен.

Сдаче экзамена подлежат студенты, по итогам семестра набравшие количество баллов, соответствующее оценке «неудовлетворительно», а также студенты, желающие повысить свою оценку.

Шкала перевода баллов в оценки:

- менее 61 балла – «неудовлетворительно»;
- от 61 до 75 баллов – «удовлетворительно»;
- от 76 до 90 баллов – «хорошо»;
- от 91 до 100 баллов – «отлично».

Преподаватель может использовать систему штрафов, уменьшая набранные баллы за пропуски занятий без уважительных причин, за нарушение сроков выполнения учебных заданий, за систематический отказ отвечать на занятиях и т.д. Возможно также начисление премиальных баллов за работы, выполненные студентом на высоком уровне.

Экзамен проводится в устно-письменной форме. Экзамен включает письменную часть – ответ по экзаменационному билету. Устная часть экзамена оценивает знания по дисциплине путём собеседования с преподавателем.

Примерные вопросы к экзамену:

1. Собственные и примесные полупроводники. Электронная и дырочная проводимости.
2. Основные параметры *p-n* перехода.
3. Полупроводниковые диоды.
4. Биполярный транзистор. Схемы включения.
5. Биполярный транзистор как четырехполюсник. *h*-параметры.
6. Полевые транзисторы.
7. Усилители электрических сигналов. Выбор рабочей точки.
8. Обратная связь в усилителях.
9. Дифференциальный усилитель.
10. Операционные усилители.
11. Применение операционных усилителей.
12. Генераторы гармонических колебаний. Принцип работы и основные параметры.
13. Транзисторные ключи.
14. Цифровые схемы. Логические элементы «И», «ИЛИ», «НЕ».
15. Сумматоры.
16. Триггеры на логических элементах.
17. Регистры.
18. Счётчики.
19. Мультиплексоры и демультиплексоры.

20. Шифраторы и дешифраторы
21. Цифро-аналоговые преобразователи.
22. Аналого-цифровые преобразователи.
23. Частотные характеристики *RC*-цепей.
24. Реакция *RC*-цепей на импульсное воздействие.
25. Спектры периодических сигналов.
26. Спектры непериодических сигналов.
27. Случайные сигналы. Шумы в электронных устройствах.
28. Модуляция и демодуляция сигналов.

Примерные контрольные вопросы к лабораторным работам

Лабораторная работа 1

- Что называется полупроводниковым диодом? Каково устройство и принцип работы диода?
- Как образуется запирающий слой в электронно-дырочном переходе и как он изменяется, если приложить к переходу прямое или обратное напряжение?
- Каково аналитическое выражение ВАХ диода? Объясните величины входящие в формулу.
- Почему обратный ток диода практически не зависит от величины обратного напряжения? Что называется током утечки? Что называется током термогенерации?
- Назовите основные виды пробоя *p-n* перехода. Что такое лавинный пробой? Что такое тепловой пробой? Как влияет температура на ВАХ?
- Каково устройство и принцип работы диода Шоттки и светодиода?

Лабораторная работа 2

- Что называется биполярным транзистором? Приведите схемотехнические обозначения биполярных транзисторов двух типов и название электродов. Нарисуйте схему включения с ОЭ.
- Принцип действия транзистора. За счет каких носителей тока в транзисторе образуются токи эмиттера, коллектора и базы $I_э, I_к, I_б$.
- Почему транзистор не будет работать при большом расстоянии между эмиттерным и коллекторным переходами?
- Приведите аналитические выражения, токов базы, и коллектора. Поясните смысл коэффициентов α и β. Приведите связь между ними.
- Приведите входные характеристики для схемы включения транзистора с ОЭ и объясните их.
- Приведите выходные характеристики для схемы включения транзистора с ОЭ. Объясните их.
- Представьте транзистор в виде четырехполюсника. Что такое *h*-параметры транзистора.

Лабораторная работа 3

- Что называется операционным усилителем?
- Каковы основные параметры операционного усилителя?
- Почему операционный усилитель, включенный без обратной связи, работает как релейный элемент?
- Какие допущения принимаются для операционного усилителя при выводе коэффициента усиления с различными обратными связями?
- Для чего применяется отрицательная обратная связь в усилителях?

- Какой знак будет иметь выходное напряжение инвертирующего усилителя, если на вход подано отрицательное напряжение?
- Что такое амплитудная и амплитудно-частотная характеристики усилителя?
- Как определить полосу пропускания усилителя?

Лабораторная работа 4

- Какие виды логики вы знаете?
- Назовите основные преимущества и недостатки КМОП-логики по сравнению с ТТЛ.
- Перечислите основные параметры логических элементов.
- Приведите структурную схему логического элемента 2И-НЕ на основе ТТЛ и КМОП-логики.
- Составьте таблицы истинности для логических элементов И-НЕ, И, ИЛИ-НЕ, ИЛИ, НЕ, Исключающее ИЛИ.
- Нарисуйте схемные обозначения трехвходовых логических элементов И-НЕ, И, ИЛИ-НЕ, ИЛИ, НЕ, Исключающее ИЛИ.
- Можно ли использовать логический элемент Исключающее ИЛИ в качестве элемента НЕ? Если да, то как; если нет, то почему?
- Что называется триггером?
- Чем отличаются последовательностные схемы от комбинационных?
- Что означает термин «запрещенная комбинация» для RS -триггера?
- При каких комбинациях входных сигналов изменяется состояние RS -триггера?

Лабораторная работа 5

- В каком положении устанавливается выход Q и $\underline{Q}$ JK -триггера после окончания синхронизирующего импульса для различных сочетаний сигналов J и K?
- Чем отличаются таблицы истинности RS и JK -триггера?
- Нарисуйте схему T-триггера, реализованную на базе JK -триггера.
- Нарисуйте схему D-триггера, реализованную на базе JK -триггера.
- На основе каких элементов строятся счетчики?
- Нарисовать схему двоичного суммирующего четырехразрядного счетчика на базе JK -триггеров.
- Чем отличаются асинхронные счетчики от синхронных? Перечислить основные преимущества синхронных счетчиков по сравнению с асинхронными.
- Сколько разрядов должен иметь двоичный счетчик, чтобы обеспечить возможность счета 64 импульсов?

Лабораторная работа 6

- Где находится рабочий участок на ВАХ стабилитрона?
- Как работает параметрический стабилизатор напряжения?
- Для чего служит балластный резистор?
- При каком минимальном напряжении на входе стабилизатора ещё возможна стабилизация напряжения?
- Как изменится напряжение на выходе стабилизатора при повышении температуры?

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОК-8: способность к самоорганизации и самообразованию	**Знать:** содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; **Уметь:** самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;	Подготовка и защита отчетов по лабораторным работам; ответы на контрольные вопросы к работам; экзаменационные вопросы.	Компетенции сформированы при правильности и полноте ответов на теоретические вопросы при защите лабораторных работ, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-5: способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	**Знать:** основные принципы работы и проектирования электронных систем; особенности применения аналоговых и цифровых радиоэлектронных устройств. **Уметь:** рассчитывать простые аналоговые и цифровые радиоэлектронные устройства.		
3.	ПК-11: способность участвовать в проведении экспериментально-исследовательских работ при проведении	**Знать:** основные параметры и принципы работы базовых аналоговых и цифровых функциональных элементов электроники. **Уметь:**		

	сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	оценивать степень достоверности результатов, полученных с помощью экспериментальных и теоретических методов исследований.		
4.	ПК-12: способность проводить инструментальный мониторинг защищенности компьютерных систем	**Знать:** основные физические понятия и принципы функционирования базовых электронных полупроводниковых компонентов в аналоговых и цифровых системах. **Уметь:** проводить базовые теоретические и экспериментальные исследования электронного оборудования и систем; оценивать степень достоверности результатов, полученных с помощью экспериментальных и теоретических методов исследований.		
5.	ПК-19: способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации	**Знать:** терминологию и символику, используемую в электронике, методы составления и чтения основных видов электрических схем; особенности применения аналоговых и цифровых радиоэлектронных устройств. **Уметь:** проводить базовые теоретические и экспериментальные исследования электронного оборудования и систем; проводить контрольные проверки работоспособности применяемых средств защиты информации.		

7. Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная литература:

1. Водовозов, А.М. Основы электроники : учеб. пособие / А.М. Водовозов. - 2-е изд. - Москва ; Вологда : Инфра-Инженерия, 2019. - 140 с. - ISBN 978-5-9729-0346-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1053394 (дата обращения: 25.04.2020).

7.2 Дополнительная литература:

1. Кучумов, Александр Иванович. Электроника и схемотехника : учеб. пособие для студ., обуч. по спец. "Компьют. безопасность" и "Комплексное обеспечение информац. безопасности автоматизир. систем" / А. И. Кучумов. 2-е изд., перераб. и доп. Москва : Гелиос АРВ, 2004. 336 с. : ил. ISBN 5-85438-099-4

2. Здыренкова, Т. В. Электротехника и электроника : учебное пособие / Т. В. Здыренкова, В. А. Михеев, В. А. Стариков ; А. Н. Животова [и др.]. — Тюмень : ТюмГУ, 2013. — 412 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110075 (дата обращения: 25.04.2020). — Режим доступа: для авториз. пользователей.

3. Шошин, Е. Л. Электроника. Полупроводниковые приборы : учебное пособие / Е. Л. Шошин. — Москва : Ай Пи Ар Медиа, 2021. — 238 с. — ISBN 978-5-4497-0508-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/100742.html (дата обращения: 24.04.2020). — Режим доступа: для авторизир. пользователей.

7.3 Интернет-ресурсы:

1. eLIBRARY – Научная электронная библиотека (Москва) http://elibrary.ru/
2. онлайн-симулятор электронных схем: https://www.easyeda.com

7.4 Современные профессиональные базы данных и информационные справочные системы:

Не предусмотрено использование в данной дисциплине.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Лицензионное ПО:

платформа для электронного обучения Microsoft Teams.

9. Технические средства и материально-техническое обеспечение дисциплины

Для проведения лекционных занятий требуется аудитория, рассчитанная на 60-80 человек, оборудованная мультимедийными средствами, а так же меловой или интерактивной доской.

Для лабораторных занятий - лаборатория со специализированным лабораторным оборудованием, аналоговые и цифровые приборы для электроизмерений.

Список оборудования для проведения лабораторных работ:

лабораторные стенды «Основы электроники», исполнение моноблочное ручное со столами-трансформерами ОЭ-МР; осциллограф С1-83; мультиметр MS-8201 H, осциллограф GOS-620FG; цифровой настольный прибор (мультиметр) для измерения силы постоянного тока, постоянного и переменного напряжения, частоты, сопротивления, емкости конденсаторов Mastech M-9803R ORIG.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

ЯЗЫКИ ПРОГРАММИРОВАНИЯ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Плотоненко Ю. А. Языки программирования Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины Языки программирования опубликована на сайте ТюмГУ: Информатика [электронный ресурс] / Режим доступа: https://www.utmn.ru/sveden/education/#

© Тюменский государственный университет, 2020.
© Плотоненко Ю. А., 2020.

1. Пояснительная записка

Программа дисциплины ориентирована на достижение следующих целей: освоение базовых конструкция языка программирования высокого уровня; изучение стандартных типов данных языка программирования высокого уровня; овладение умением конструирования пользовательских типов данных; получение знаний о приёмах алгоритмизации, о формальной постановке задачи, об основных этапах реализации программ на компьютере; формирование готовности использовать приобретенные знания в профессиональной деятельности.

Задачи дисциплины:

- получение знаний, составляющих основу научных представлений об информации, информационных процессах, системах, технологиях и моделях; приобретении практических навыков работы с различными видами информации с помощью компьютера и других средств информационных и коммуникационных технологий;
- обучение студентов основным подходам к проектированию, разработке и использованию программ;
- дать обучающимся знание технологий разработки программного обеспечения с использованием универсальных языков программирования.

1.1. Место дисциплины *(модуля)* в структуре образовательной программы

Данная дисциплина входит в блок Б1, Базовая часть. Дисциплина «Языки программирования» базируется на знаниях курсов «Информатика», «Алгебра и геометрия» школы. Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться при изучении курсов численных методов, вычислительного практикума, при выполнении курсовых и дипломных работ, связанных с математическим моделированием и обработкой наборов данных.

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля)*

Код и наименование компетенции	Код и наименование части компетенции (при наличии паспорта компетенций)	Компонент (знаниевый/функциональный)
ОПК-8: способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач.		Знает: основные направления развития технологий программирования, виды основных структур данных, их особенности, основные методы решения типовых численных задач, методы решения профессиональных, исследовательских и прикладных задач. Умеет: формализовать вычислительную задачу и выбрать необходимый типовой алгоритм для ее решения; выявить типовые, а также нестандартные задачи, разработать метод решения поставленной задачи с использованием типовых алгоритмов.
ОПК-10: способностью к самостоятельному построению алгоритма,		Знает: основные концептуальные положения процедурного программирования, основные методы

проведению его анализа и реализации в современных программных комплексах.		реализации соответствующих алгоритмов с помощью ЭВМ; алгоритмы и технологии программирования для разработки приложений, осуществляющих решение типовых задач. Умеет: разрабатывать специализированные программы для решения задач, тестировать и отлаживать программы в интегрированной среде разработки; опираясь на знания теоретических основ программирования, оптимизировать исходный код.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Часов в семестре**		
			2	3	4
Общая трудоемкость	**зач. ед.**	13	4	4	5
	час	468	156	156	156
Из них:					
Часы аудиторной работы (всего):		216	72	72	72
Лекции		108	36	36	36
Практические занятия		0	0	0	0
Лабораторные / практические занятия по подгруппам		108	36	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося		252	84	84	84
Вид промежуточной аттестации (экзамен, зачет)			Экзамен	Зачет	Экзамен

3. Система оценивания

Оценивание знаний, умений и навыков студентов, полученных ими в ходе изучения дисциплины, производится в соответствии с «Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся Федерального государственного автономного образовательного учреждения высшего профессионального образования «Тюменский государственный университет»» (утверждено решением Ученого совета, протокол № 10 от 31.08.2020 г.). В соответствии с Положением, все виды работ студента, выполняемые в течение семестра (ответы на теоретические вопросы, самостоятельное выполнение практических заданий, подготовка сообщений на заданные темы, самостоятельное изучение дополнительных глав дисциплины), оцениваются в баллах. Результаты текущего контроля заносятся в информационную систему поддержки учебного процесса.

3.1. Система текущего контроля

В процессе текущего контроля оценивается качество выполнения студентом задания практикума и ответов на вопросы собеседования в рамках защиты выполненных заданий (с учетом их сложности).

Шкала оценивания при проведении ***текущего контроля***:

0 баллов – задание не выполнено.
2 балла – при выполнении задания и ответе на вопрос допущены существенные ошибки.
4 баллов – выполнение задания с несущественными ошибками, неполный ответ на вопрос.
6 баллов – выполнение без ошибок в соответствии с заданием, полный ответ на вопрос.

3.2. Система промежуточного оценивания:

Промежуточное оценивание производится по итогам завершения первой половины дисциплины на зачёте в конце 3-го семестра. Оценка студента на зачёте является интегрированной оценкой выполнения студентом заданий во время практических занятий и ответов на вопросы. Эта оценка характеризует уровень сформированности умений и навыков, приобретенных студентом в ходе изучения первой половины дисциплины.

Студент получает зачёт автоматически в случае набора в течение третьего семестра 61 балла или более.

Если студент набирает в течение семестра менее 61 балла, то он должен явиться на зачёт. Зачёт проводится в форме выполнения практических заданий и собеседования. Зачётный билет содержит две практические задачи на разные темы из разделов 3 семестра.

Если студент набирает в течение семестра менее 35 баллов, то он также должен явиться на зачёт. Зачёт проводится в устно-письменной форме. Зачётный билет содержит две практические задачи на разные темы из разделов первой половины курса. Кроме заданий билета студенту задаются дополнительные вопросы по несданным разделам дисциплины.

Оценка выставляется по итогам полноты решения практического задания и ответа на дополнительные вопросы.

Ответ на каждое из заданий билета к зачёту оценивается по следующей шкале:

«не зачтено» – задача не решена или в ней реализовано менее 70% требуемого функционала.

«зачтено» – практическое задание выполнено на 70% и более.

Итоговая оценка выводится как «зачтено» если зачтены оба задания практической части билета и студент достойно ответил на большинство вопросов.

3.3. Система итогового оценивания:

Экзаменационная оценка студента является интегрированной оценкой выполнения студентом заданий во время практических занятий и ответов на вопросы. Эта оценка характеризует уровень сформированности умений и навыков, приобретенных студентом в ходе изучения дисциплины.

Студент получает экзамен автоматически в случае набора в течение последнего семестра изучения дисциплины количества баллов:

61 – 75 баллов – «удовлетворительно»;

76 – 90 баллов – «хорошо»;

91 – 100 баллов – «отлично».

Студент набирает в течение семестра менее 61 балла. В этом случае студент должен явиться на экзамен. Экзамен проводится в устно-письменной форме. Билет содержит 2 вопроса из разных разделов двухсеместрового курса и одну практическую задачу.

Студент набирает в течение семестра менее 35 баллов. В этом случае студент также должен явиться на экзамен. Экзамен проводится в устно-письменной форме. Билет содержит 2 вопроса из разных разделов курса и 2 практических задачи. Кроме вопросов билета студенту задаются дополнительные вопросы по несданным разделам дисциплины. Оценка выставляется по итогам ответа на экзаменационный вопрос и ответа на дополнительные вопросы.

Студент, желающий исправить экзаменационную оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена. Экзамен проводится в устно-письменной форме. Билет содержит 2 вопроса из разных разделов курса и 2 практических задачи. В случае, если студент отказывается от сдачи экзамена или не смог повысить оценку, ему выставляется оценка, полученная автоматически по итогам семестра.

Ответ на каждый из вопросов экзаменационного билета оценивается по следующей шкале:

2 («неудовлетворительно») - студент не ответил на вопрос либо содержание ответа не раскрывает сути вопроса.

3 («удовлетворительно») - студент отвечает по существу, но не демонстрирует целостного представления по вопросу, не может аргументировать свой ответ.

4 («хорошо») - студент отвечает по существу, демонстрирует целостное представление по вопросу; не может аргументировать свой ответ либо аргументация не обоснована.

5 («отлично») - студент дает полный, развернутый, аргументированный ответ на вопрос.

Итоговая оценка выводится как средняя арифметическая из оценок по всем трём позициям билета.

Примечание.
Участие в олимпиадах/конкурсах/чемпионатах по программированию: за призовое место (уровень не ниже университетского) текущий рейтинг может быть повышен на 5-10 баллов.

4. Содержание дисциплины
4.1. Тематический план дисциплины

Таблица 2

№	Наименование тем и/или разделов	Объем дисциплины (модуля), час				
		Всего	Виды аудиторной работы (в час.)			
			Лекции	Практические занятия	Лабораторные / Практические занятия по подгруппам	Иные виды контактной работы
1	2	3	4	5	6	7
2 семестр						
1.	Введение в C#. Система типов языка C#. Выражения и операторы. Управление действиями с данными. Массивы.	30	8	0	6	0
2.	Основные принципы и этапы ООП. Классы и объекты. Элементы класса. Поля и методы. Свойства объектов.	26	6	0	6	0
3.	Наследование в C#.	34	8	0	8	0
4.	Виртуальные и динамические методы. Полиморфизм.	32	6	0	8	0
5.	Абстрактные классы. Интерфейсы. Исключения. Делегаты и события	34	8	0	8	0
	Итого за семестр	156	36	0	36	2

3 семестр						
6.	Основы визуального программирования на языке C#.	26	6	0	6	0
7.	Использование стандартных компонент пользовательского интерфейса	34	8	0	8	0
8.	Разработка многооконных приложений. Стандартные окна диалога. Файловые типы данных.	44	10	0	10	0
9.	Организация механизма Drag&Drop.	18	4	0	4	0
10.	Построение графических изображений.	34	8	0	8	0
	Итого за семестр	156	36	0	36	0
4 семестр						
11.	Организация многопоточных приложений.	16	4	0	4	0
12.	Основы языка Python.	28	8	0	4	0
13.	Организация работы с файлами в Python.	16	4	0	4	0
14.	Функции в Python.	22	4	0	6	0
15.	Основы ООП в Python.	34	8	0	8	0
16.	Технологии доступа к данным.	56	12		14	
	Итого за семестр	156	36	0	36	2
	Итого (часов)	**468**	**108**	**0**	**108**	**4**

4.2. Содержание дисциплины по темам

Все практические работы требуют разработку оконного приложения, которое реализует поставленные задачи и имеет пользовательский интерфейс для управления параметрами задания. Задания практикума выполняются с использованием системы программирования Microsoft Visual Studio.

Тема 1. Введение в C#. Система типов языка C#. Выражения и операторы. Управление действиями с данными. Массивы.

Характеристика языка C#; сравнительный анализ языков C++, C#, Pascal; структура программы на C#; организация ввода-вывода в консольном приложении. Система типов языка C#. Встроенные типы данных, преобразование типов; типы-значения и ссылочные типы; упаковка и распаковка. Литералы и переменные. Литералы разных типов; переменные и их инициализация; область видимости и время жизни переменных. Выражения и операторы. Арифметические операторы; логические операторы; приоритет операций; преобразование типов в выражениях. Управление действиями с данными. Оператор присваивания; операторы

условный и выбора; операторы цикла; операторы перехода. Создание и инициализация массивов; ступенчатые массивы; класс Array (основные свойства и методы).

Практическая работа по подгруппам 1.

Разработка консольных приложений в среде в стиле структурного программирования.

Тема 2. Основные принципы и этапы ООП. Классы и объекты. Элементы класса. Поля и методы. Свойства объектов.

Принципы абстрагирования, ограниченного доступа, модульности, иерархичности, типизации, параллелизма, устойчивости. Обзор этапов разработки программного обеспечение в стиле ООП. Принципы абстрагирования, ограниченного доступа, модульности, иерархичности, типизации, параллелизма, устойчивости. Обзор этапов разработки программного обеспечение в стиле ООП. Объектная декомпозиция. Объектные сообщения, классы. Средства разработки и описания классов. Ограничение доступа. Принцип инкапсуляции. Организация свойств. Защита данных. Индексаторы.

Практическая работа по подгруппам 2.

Разработка макетов классов. Выделение элементов классов, разграничение зон их функционирования. Разработка консольного приложения в стиле объектно-ориентированного программирования.

Практическая работа по подгруппам 3.

Описание классов, создание объектов, управление объектами. Построение консольных приложений с использованием классов. Оформление полей и методов. Перегрузка операций.

Тема 3. Наследование в C#.

Производные классы, конструкторы и наследование; преобразование типов при работе с иерархией объектов; операторы проверки и приведения типа. Вида наследования. Изменение видимости элементов класса при наследовании.

Практическая работа по подгруппам 4.

Построение консольных приложений с использованием классов. Оформление полей и методов. Реализация принципа наследования. Разработка конструкторов и деструкторов.

Тема 4. Виртуальные и динамические методы. Полиморфизм.

Принцип полиморфизма. Раннее и позднее связывание. Особенности виртуальных методов. Горизонтальный и вертикальный полиморфизм. Функционирование полиморфных объектов.

Практическая работа по подгруппам 5.

Построение консольных приложений с учётом реализации принципа полиморфизма. Реализация горизонтального и вертикального полиморфизма. Организация семейства полиморфных объектов.

Тема 5. Абстрактные классы. Интерфейсы. Исключения. Делегаты и события

Абстрактные классы и наследование; абстрактный класс Object. Интерфейсы. Реализация интерфейсов; интерфейсы и классы; интерфейсы и структуры. Исключения. Обработка исключений, генерация исключений; класс Exception; исключения и наследование. Функциональный тип. Два способа взаимодействия частей при построении сложных систем. Функции обратного вызова. Наследование и функциональные типы. Класс Delegate. Методы и свойства класса. Операции над делегатами. Комбинирование делегатов. Список вызовов. Делегаты и события. Классы с событиями, допускаемые .Net Framework. Класс EventArgs и его потомки. Связывание обработчика с событием.

Практическая работа по подгруппам 6.

Разработка приложений с использованием абстрактных классов и интерфейсов.

Практическая работа по подгруппам 7.

Построение консольных приложений с использованием событийного программирования. Применение стандартных и пользовательских делегатов.

Тема 6. Основы визуального программирования на языке C#.

Форма. Размещение компонентов на макете. Окно настройки параметров компонентов.

Практическая работа по подгруппам 8.

Разработка простейших приложений for Windows.

Тема 7. Использование стандартных компонент пользовательского интерфейса

Размещение компонентов на макете. Окно настройки параметров компонентов. Общие свойства и общие события компонентов. Взаимодействие элементов управления, элементов ввода-вывода данных различного типа друг с другом.

Практическая работа по подгруппам 9.

Разработка оконных приложений, включающих базовые элементы пользовательского интерфейса (форму, кнопки), с динамическим управлением свойствами визуальных компонент и обработкой многочисленных пользовательских событий.

Практическая работа по подгруппам 10.

Разработка оконных приложений, включающих базовые элементы пользовательского интерфейса (форму, кнопки, надписи, окна ввода), с динамическим управлением свойствами визуальных компонент и обработкой многочисленных пользовательских событий.

Тема 8. Разработка многооконных приложений. Стандартные окна диалога. Файловые типы данных.

Принципы разработки приложений в стиле SDI и MDI интерфейсов. Модальные формы. Организация диалоговых окон. Стандартные окна диалога. Файлы. Создание потоков. Текстовые, битовые, xml файлы.

Практическая работа по подгруппам 11.

Разработка приложений для работы с файлами. Разработка приложений со стандартными и пользовательскими диалоговыми окнами.

Практическая работа по подгруппам 12.

Разработка многооконных приложений с использованием SDI и MDI интерфейсов.

Тема 9. Организация механизма Drag&Drop

Основные события, механизмы интерфейса Drag&Drop. Организация интерфейса Drag&Drop для передачи данных и запросов.

Практическая работа по подгруппам 13.

Разработка оконного приложения, управление настройками и контентом которого осуществляется посредством механизма Drag&Drop.

Тема 10. Построение графических изображений

Контекст устройства Windows, интерфейс GDI+. Класс Graphics. Графические примитивы, инструменты для их настройки и применения. Работа с готовыми изображениями. Классы и компоненты, предназначенные для работы с графикой.

Практическая работа по подгруппам 14.

Разработка оконного приложения, позволяющего строить, настраивать, обрабатывать, сохранять статические и динамический изображения с использованием различных графических инструментов.

Тема 11. Организация многопоточных приложений.

Принципы организации вытесняющей многозадачности. Класс Thread. Создание и разрушение потоков. Управление потоками. Параметризованный вызов метода. Обмен данными с потоком. Особенности многопоточности в оконных приложениях.

Практическая работа по подгруппам 15.

Разработка консольного и оконного приложений, включающих организацию многопоточности при выполнении расчётов и при обслуживании пользовательского интерфейса.

Тема 12. Основы языка Python.

Язык программирования Python. Особенности языка. Понятие текстового редактора и компилятора. Запуск программ. Архитектура хранения информации в компьютере. Основные типы объектов в языке Python:списки, кортежи, словари. Упаковка данных. Специфика хранения типов данных. Основные арифметические операции и их реализация в Python: сложение, умножение, вычитание, деления, возведение в степень, нахождение остатка от деления нацело. Синтаксис операций. Результат выполнения операций с использованием различных типов объектов. Особенности при использовании в прикладных экономических задачах. Функции print, input. Синтаксис функций. Управляющие последовательности в функциях. Формат введенного пользователем числа. Конструкция выбора if-else, if-elif. Синтаксис использования конструкции. Логические операции в конструкции. Последовательность операций сравнения. Конструкция циклов do-while, while, for. Синтаксис использования конструкций. Логические операции в конструкции. Последовательность операций сравнения. Понятие одномерного и двумерного списка. Формирование списков. Присваивание значений элементам списка. Операции над списками. Вывод элементов списка на экран и в файл. Использование списков для хранения данных.

Практическая работа по подгруппам 16.

Разработка приложений реализующие основные конструкции языка программирования Python. Использование строк и списков.

Тема 13. Организация работы с файлами в Python.

Чтение из текстового файла. Основные методы чтения. Режимы чтения. Специфика кодировки. Конструкция try-except-else. Обработка исключений. Работа с курсором. Запись в файл. Режим открытия файлов.

Практическая работа по подгруппам 17.

Разработка приложений для работы с файлами.

Тема 14. Функции в Python.

Синтаксис задания функций. Объявление функций. Тип функции. Тело функции. Функции, которые не возвращают значение. Функция в функции. Использование функций в экономических задачах.

Практическая работа по подгруппам 18.

Разработка приложений с использованием функций.

Тема 15. Основы ООП в Python.

Классы и объекты в языке программирования Python, элементы класса, свойства, методы, параметры методов, перегрузка методов. Создание и разрушение объектов. Конструкторы и инициализация данных, деструкторы.

Практическая работа по подгруппам 19.

Разработка приложений с использованием классов.

Тема 16. Технологии доступа к данным.

Структура, механизм и компоненты ADO.Net.

Практическая работа по подгруппам 20.

Создание приложений, использующих технологию ADO.NET.

Средство проведения текущего контроля – тестирование разработанного программного продукта для различных режимов и настроек работы и собеседование по теоретическим вопросам данной темы.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ Темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Введение в C#. Система типов языка C#. Выражения и операторы. Управление действиями с данными. Массивы.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
2.	Основные принципы и этапы ООП. Классы и объекты. Элементы класса. Поля и методы. Свойства объектов.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
3.	Наследование в C#.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
4.	Виртуальные и динамические методы. Полиморфизм.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
5.	Абстрактные классы. Интерфейсы. Исключения. Делегаты и события	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
	Промежуточная аттестация	**Подготовка к промежуточной аттестации (экзамену)**
6.	Основы визуального программирования на языке C#.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
7.	Использование стандартных компонент пользовательского интерфейса	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
8.	Разработка многооконных приложений. Стандартные окна диалога. Файловые типы данных.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.

9.	Организация механизма Drag&Drop.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
10.	Построение графических изображений.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
	Промежуточная аттестация	**Подготовка к промежуточной аттестации (зачёту)**
11.	Организация многопоточных приложений.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
12.	Основы языка Python.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
13.	Организация работы с файлами в Python.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
14.	Функции в Python.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
15.	Основы ООП в Python.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
16.	Технология доступа к данным.	Работа с учебной литературой. Разработка алгоритмов реализации практического задания. Написание и отладка программы.
	Промежуточная аттестация	**Подготовка к промежуточной аттестации (экзамену)**

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение основной и дополнительной литературы.
3. Разбор примеров для аналогичных заданий.
4. Разработка собственного алгоритма для конкретного задания.
5. Программная реализация алгоритма.
6. Отладка приложения на тестовых примерах.

При подготовке к промежуточной аттестации (к зачёту) студент отрабатывает навыки разработки объекто-ориентированных приложений и готовится к теоретическим вопросам по пройденным темам при объяснении разработанных программ.

6. Промежуточная аттестация по дисциплине

6.1 Оценочные материалы для проведения промежуточной аттестации по дисциплине

Форма промежуточной аттестации – зачёт.

Экзамен проводится в виде решения двух практической заданий, состоящих в написании программных приложений и собеседования по разработанным программам и изученным темам.

Пример зачетного билета:

1. На форме расположены ListBox1, Label1 и Button1. В ListBox1 записаны целые числа. При нажатии на кнопку необходимо определить среди выделенных элементов среднее значение всех нечетных отрицательных чисел. Результат вывести в Label1.

Напишите соответствующий обработчик события Click для кнопки Button1:

```
private void button1_Click(object sender, EventArgs e)
    {       }
```

Задание 2

На форме расположены ListBox1, ListBox2, OpenFileDialog1, Button1 и Button2. При нажатии на первую кнопку открывается окно диалога для выбора файла. После выбора текстового файла его содержимое загружается в ListBox1. При нажатии на вторую кнопку все строки имеющие английские буквы переносятся в ListBox2.

Напишите соответствующие обработчики события Click для Button1 и Button2:

```
private void button1_Click(object sender, EventArgs e)
    {       }
private void button2_Click(object sender, EventArgs e)
    {       }
```

Форма проведения второй промежуточной аттестации – экзамен. Экзамен проводится в виде собеседования по теоретическим вопросам экзаменационного билета и написания программы по темам дисциплины.

Пример экзаменационного билета: Экзаменационный билет содержит 2 теоретических вопроса из списка примерных вопросов и 2 практических задания, связанное с содержанием теоретического вопросов к курсу.

1. (Язык программирования Python) Написать модуль, содержащий описание следующего класса:

Поля:

- фамилия и инициалы;
- номер группы;
- успеваемость (список из пяти элементов).

Содержание класса:

- поля, свойства, методы;
- все поля класса должны быть приватными;
- реализовать конструктор и деструктор;
- свойства по изменению и отображению значения полей;
- метод поиска информации из списка объектов по определенным критериям;
- переопределенный метод __str__() для вывода информации об бъекте.

2. (Язык программирования C#) Имеется форма на которой расположены следующие компоненты:

- TextBox1,
- ListBox1,
- Button1 и Button2.

a) Написать обработчик события Click для кнопки Button1 позволяющей добавлять элементы из TextBox1 в ListBox1.

b) Написать обработчик события Click для кнопки Button2 позволяющей определить все четные числа кратные 6 среди выделенных элементов в ListBox1.

3. (Язык программирования C#) Технология Drag&Drop (начало перетаскивания, определение возможности передачи приемнику перетаскиваемого элемента, бросание элемента, завершение операции, класс DataObject, класс DataFormats, метод DoDragDrop).

4. (Язык программирования Python) Объектно-ориентированное программирование (наследование, инкапсуляция, класс object, строковое представление объекта, методы).

Примерный перечень вопросов теоретической части:

2. Язык программирования C#.
    1. Основы языка C# (Комментарии, литералы, переменные, их инициализация, область видимости и время жизни переменных. Типы данных в языке C# . Ввод и вывод в C#. Форматирование вывода.)
    2. Массивы в C# (Описание массивов, одномерные и многомерные массивы).
    3. Операторы в C# (Оператор присваивания, преобразования типа в операциях присваивания. Выполнение операции приведения типа между несовместимыми типами данных, Преобразование типов в выражениях. Операторы if и switch. Операторы цикла.).
    4. Понятие объектно-ориентированного программирования. Абстракция, наследование, инкапсуляция, полиморфизм.
    5. Классы. Объявление класса; элементы класса: данные-члены (переменные экземпляра, статические переменные, константы, события), функции-члены (методы, конструкторы, деструкторы, индексаторы, операторы (операции), свойства), вложенные типы. Объявление и использование перегруженных операторов, свойств и индексаторов.
    6. Объявление и реализация методов, параметры методов. Перегрузка методов. Виртуальные методы. Переопределение методов.
    7. Создание объектов. Объявление, реализация и вызов конструкторов. Вызов конструктора наследуемого класса. Деструкторы. Сборка мусора в C#.
    8. Реализация наследования в C#. Объявление производных классов, использование правил преобразования типов при работе с иерархией объектов; использование операторов проверки и приведения типа.
    9. Абстрактные классы. Использование абстрактных классов. Абстрактный класс object. Интерфейсы. Способы реализации интерфейсов.
    10. Исключения. Обработка исключений, генерация исключений; класс Exception; программирование алгоритмов с использованием исключений.
    11. Делегаты и события. Примеры создания и использования делегатов. Многоадресные делегаты. Определение и использование событий; стандартные и пользовательские события в приложениях. Широковещательные события.
    12. Визуальное программирование. Класс Application. Класс Form. События клавиатуры. События мыши.
    13. Компоненты управления (Label, TextBox, Button, CheckBox, RadioButton, GroupBox, Panel, ListBox, CheckListBox, ComboBox, NumericUpDown, ProgressBar, TrackBar, главное (головное) меню, контекстное (всплывающее) меню, Timer, PictureBox, ToolTip, RichTextBox, ErrorProvider).
    14. Стандартные диалоги (FontDialog, ColorDialog, FolderBrowserDialog, OpenFileDialog, SaveFileDialog).
    15. Создание компонентов в коде. Добавление элементов управления в режиме работы приложения. Управление буфером обмена Класс Clipboard.
    16. Технология Drag&Drop (начало перетаскивания, определение возможности передачи приемнику перетаскиваемого элемента, бросание элемента, завершение операции, класс DataObject, класс DataFormats, метод DoDragDrop, перечисление DragDropEffects, класс DragEventArgs, класс GiveFeedbackEventArgs, класс QueryContinueDragEventArgs, события операции Drag&Drop).
    17. Файлы. Создание потоков. Текстовые, битовые, xml файлы.
    18. Работа с формами. (параллельные формы (SDI), модальные формы, многодокументный интерфейс (MDI), поверх всех окон, собственные формы, пользовательские (композитные) формы).
    19. Графические инструменты. Класс Graphics, методы класса. Карандаш Pen. Кисть Brush.

20. Технология доступа к данным ADO.NET. Модель ADO.NET. Провайдеры данных. Класс DataSet. Класс DataTable. Класс DataView. Класс OleDbConnection. Класс DataAdapter. Класс OleDbCommand. Класс OleDbParameterCollection. Класс OleDbParameter. Использование XML в DataSet.
21. Многопоточное программирование. Архитектура параллельного программирования в .NET Framework. Класс Thread. Класс Task. Класс Parallel.

2. Язык программирования Python.
22. Основы python (переменные, типы данных, операции, выражения, условная конструкция if, циклы).
23. Списки, кортежи, словари, множества.
24. Строки (работа со строками, методы, форматирование строки).
25. Работа с файлами (открытие и закрытие файлов, текстовые файлы, бинарные файлы, файлы csv).
26. Синтаксис задания функций. Объявление функций. Тип функции. Тело функции. Функции, которые не возвращают значение. Функция в функции. Использование функций в экономических задачах.
27. Объектно-ориентированное программирование (классы и объекты, конструкторы, деструкторы, свойства, методы, наследование, инкапсуляция, полиморфизм, класс object, строковое представление объекта)

6.2 Критерии оценивания компетенций:

Таблица 4

Карта критериев оценивания компетенций

№ п/п	Код и наимено-вание компетенции	Критерии оценивания	Оценочные материалы	Критерии оценивания
1	ОПК-8: способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач.	Знает: основные направления развития технологий программирования, виды основных структур данных, их особенности, основные методы решения типовых численных задач, методы решения профессиональных, исследовательских и прикладных задач. Умеет: формализовать вычислительную задачу и выбрать необходимый типовой алгоритм для ее решения; выявить типовые, а также нестандартные задачи, разработать метод решения поставленной задачи с использованием типовых алгоритмов.	Собеседование по теме практической работы по подгруппам, Зачет, Экзамен	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев согласно требованиям п.4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2	ОПК-10: способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в	Знает: основные концептуальные положения процедурного программирования, основные методы реализации соответствующих алгоритмов с помощью ЭВМ; алгоритмы и технологии программирования для	Собеседование по теме практической работы по подгруппам, Зачет, Экзамен	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий.

	современных программных комплексах.	разработки приложений, осуществляющих решение типовых задач. Умеет: разрабатывать специализированные программы для решения задач, тестировать и отлаживать программы в интегрированной среде разработки; опираясь на знания теоретических основ программирования, оптимизировать исходный код.		Шкала критериев согласно требованиям п.4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература:

1. Маляров, А. Н. Объектно-ориентированное программирование : учебник для технических вузов / А. Н. Маляров. — Самара : Самарский государственный технический университет, ЭБС АСВ, 2017. — 332 с. — ISBN 978-5-7964-1952-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91772.html (дата обращения: 25.05.2020).

7.2 Дополнительная литература:

1. Биллиг, В. А. Основы программирования на C# : учебное пособие / В. А. Биллиг. — 2-е изд. — Москва : ИНТУИТ, 2016. — 574 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100319 (дата обращения: 25.05.2020).
2. Сузи, Р. А. Язык программирования Python : учебное пособие / Р. А. Сузи. — 2-е изд. — Москва : ИНТУИТ, 2016. — 350 с. — ISBN 5-9556-0058-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100546 (дата обращения: 01.05.2020). — Режим доступа: для авториз. пользователей.
3. Северенс, Ч. Введение в программирование на Python : учебное пособие / Ч. Северенс. — 2-е изд. — Москва : ИНТУИТ, 2016. — 231 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100703 (дата обращения: 01.05.2020). — Режим доступа: для авториз. пользователей.
4. Хахаев, И. А. Практикум по алгоритмизации и программированию на Python : учебное пособие / И. А. Хахаев. — 2-е изд. — Москва : ИНТУИТ, 2016. — 178 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100377 (дата обращения: 01.05.2020). — Режим доступа: для авториз. пользователей.

7.3 Интернет-ресурсы:

1. Электронно-библиотечная система издательства «Инфра». - URL: http://znanium.com.
2. eLIBRARY – Научная электронная библиотека (Москва). - URL: http://elibrary.ru

7.4 Современные профессиональные базы данных и информационные справочные системы:

- Межвузовская электронная библиотека (МЭБ). - URL: https://icdlib.nspu.ru/
- Национальная электронная библиотека. - URL: https://rusneb.ru/
- Institute of Electrical and Electronics Engineers, Inc (IEEE). - URL: https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине:

Интернет, доступ в информационно-образовательную среду ТюмГУ, включающую в себя доступ к учебным планам и рабочим программам, к изданиям электронной библиотечной

системы и электронным образовательным ресурсам.

- Лицензионное ПО:
  - Платформа для электронного обучения Microsoft Teams
  - Microsoft Imagine Academy (ранее Dreamspark): MS Visual Studio, MS SQL Server, ОС семейства MS Windows, MS Visio, MS Project
  - Microsoft Office 365
- Свободно распространяемое ПО:
  - Программная платформа Moodle https://docs.moodle.org/dev/License
  - Дистрибутив Python Anaconda https://www.anaconda.com/eula-anaconda-individual-edition
  - Облачный сервис, предназначенный для программирования на языке Python https://colab.research.google.com

Для проведения лекционных занятий используется техническое оборудование (проектор, микрофон, камера).
Доступ к компьютерным системам осуществляется на основе договоров ТюмГУ с создателями через компьютерную сеть университета (ЭБД, ЭБС, ЭБ), либо через виртуальные читальные залы университета, в частности, читальный зал для преподавателей и аспирантов ИБЦ (ЭБД РГБ).
Доступ к информационной образовательной среде осуществляется через локальную сеть ТюмГУ.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Для чтения лекций используется аудитория, оборудованная мультимедиа проектором и персональным компьютером. Для выполнения практических заданий и самостоятельной работы используется компьютерное оборудование (персональные компьютеры с подключением к Интернету).

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

БЕЗОПАСНОСТЬ РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Оленников А.А. Безопасность распределенных компьютерных систем. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Безопасность распределенных компьютерных систем [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Оленников А.А., 2020.

1. Пояснительная записка

Учебная дисциплина «Безопасность распределенных компьютерных систем» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Целью дисциплины «Безопасность распределенных компьютерных систем» является обучение студентов основам проектирования защищенных автоматизированных систем, ознакомление с оборудованием и организации защиты датчиков, автоматизированных узлов и диспетчерских.

Задачи дисциплины «Безопасность распределенных компьютерных систем»:

- изучить современные технологические процессы и их технологию;
- основную нормативно-техническую документацию;
- изучить виды оборудования и принципы работы;
- изучить всевозможные угрозы, влияющие на работу оборудования и технологического процесса в целом;
- научиться строить модели нарушителя для предложенной технологической линейки или технологии;
- научиться настраивать оборудование;
- научиться строить принципиальные и подробные электрические схемы, в том числе с использованием эмуляторов и имитационных тренажеров;
- научиться разрабатывать мнемосхемы и скада системы для предложенного технологического процесса.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в базовую часть цикла естественно - научных дисциплин, блок Б1 Вариативная часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Сети и системы передачи информации», «Языки программирования», «Операционные системы», «Разработка и защита web приложений».

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ПК-8 – способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы.	-----	**Знать:** нормативно-техническую документацию; принцип работы оборудования автоматизированных систем; программное обеспечение для проектирования схем автоматизированных систем и узлов. **Уметь:** нормативно-техническую документацию; принцип работы оборудования автоматизированных систем; программное обеспечение для проектирования схем автоматизированных систем и узлов.

* не предусмотрено

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	Всего часов (академические часы)	Часов в семестре (академические часы)
		10 семестр
Общий объем зач. ед.	4	4
час.	144	144
Из них:		
Часы аудиторной работы (всего):	72	72
Лекции	36	36
Практические занятия	0	0
Лабораторные/практические занятия по подгруппам	36	36
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	72	72
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		экзамен

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной) и традиционной (5-балльной) систем оценок.

В 10 семестре предусмотрен экзамен. Экзаменационная оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических работ, индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должно быть выполнено минимум 50% практических работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 75% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить экзаменационную оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Введение. Обзор современных автоматизированных систем и устройств.	10	2	0	2	0
2.	Система теплоснабжения зданий различного назначения. Учет и регулировка теплоносителя.	16	4	0	2	0
3.	Тепловые счетчики, их устройство и режимы работы.	8	2	0	2	0
4.	Интерфейсы RS-232, RS-422 и RS-485.	8	2	0	0	0
5.	Система погодного регулирования. Система управления газовыми и твердотопливными котлами.	16	2	0	6	0
6.	ТРМ32 контроллер для отопления и ГВС. СУНА-121 контроллер для групп насосов. Угрозы и аварийные ситуации.	10	2	0	2	0
7.	Установки и устройства для поддержания микроклимата в помещениях/зданиях различного назначения. Модели угроз.	4	2	0	0	0
8.	Системы охранно-пожарной сигнализации и пожаротушения. Организация диспетчерских пультов.	4	4	0	0	0

9.	Системы видеонаблюдения. Проектирование сетей охранного телевидения. Виды оборудования. Защита данных.	16	2	0	4	0
10.	Системы диспетчеризации. Их обустройство. Принципиальные схемы.	8	2	0	0	0
11.	Среда проектирования Codesys. Алгоритмы работы контроллера ПЛК-150.	12	4	0	4	0
12.	Принципы конфигурирования оборудования автоматизации.	8	2	0	4	0
13.	Моделирование сетей и узлов систем автоматизации в различных средах. Имитационные модели.	8	2	0	4	0
14.	Разработка Скада-систем.	16	4	0	6	0
	Итого (часов)	144	36	0	36	2

4.2. Содержание дисциплины (*модуля*) по темам

Тема 1. Введение. Обзор современных автоматизированных систем и устройств.
Практическая работа 1. Построение структурных схем.
Необходимо изучить ГОСТ «Автоматизация технологических процессов» и построить структурные электрические схемы узлов автоматизации.
Тема 2. Система теплоснабжения зданий различного назначения. Учет и регулировка теплоносителя.
Практическая работа 2. Подбор датчиков и контроллера узла учета тепловой энергии.
Используя исходные данные согласно варианту, выполнить подбор оборудования компании «ВЗЛЕТ» для узла учета тепловой энергии. Технологический чертеж ИТП предоставляется преподавателем и является общим для всех вариантов.
Тема 3. Тепловые счетчики, их устройство и режимы работы.
Практическая работа 3. Работа с тепловычислителем ТСР-010.
Необходимо осуществить подключение к тепловычислителю и выполнитеь необходимые настройки.
Тема 4. Интерфейсы RS-232, RS-422 и RS-485.
Тема 5. Система погодного регулирования. Система управления газовыми и твердотопливными котлами.
Практическая работа 4. Разработка модели угроз системы погодного регулирования.
Необходимо изучить предложенную технологию и разработать модели угроз.
Практическая работа 5. Разработка алгоритмов и мероприятий по безаварийной работе теплового системы погодного регулирования и тепловычислителя.
Тема 6. ТРМ32 контроллер для отопления и ГВС. СУНА-121 контроллер для групп насосов. Угрозы и аварийные ситуации.
Практическая работа 6. Настройка контроллера СУНА на требуемые режимы работы.
Необходимо выполнить настройку контроллера СУНА на требуемые режимы работы.

Тема 7. Установки и устройства для поддержания микроклимата в помещениях/зданиях различного назначения. Модели угроз.
Тема 8. Системы охранно-пожарной сигнализации и пожаротушения. Организация диспетчерских пультов.
Тема 9. Системы видеонаблюдения. Проектирование сетей охранного телевидения. Виды оборудования. Защита данных.
Практическая работа 7. Работа с адресной видеокамерой и видеорегистратором, и их настройками.
Необходимо выполнить настройку цифровой видеокамеры и видеорегистратора, и организовать защиту данных.
Тема 10. Системы диспетчеризации. Их обустройство. Принципиальные схемы.
Тема 11. Среда проектирования Codesys. Алгоритмы работы контроллера ПЛК-150.
Практическая работа 8. Работа в среда проектирования Codesys.
Необходимо ознакомится со средой проектирования Codesys и разработать конфигурацию для предложенной технологии.
Тема 12. Принципы конфигурирования оборудования автоматизации.
Практическая работа 9. Работа в среда проектирования Codesys.
Необходимо ознакомится со средой проектирования Codesys и разработать конфигурацию для предложенной технологии.
Тема 13. Моделирование сетей и узлов систем автоматизации в различных средах. Имитационные модели.
Практическая работа 10. Построение и защита технологической сети.
В среде автоматизированной разработки схем необходимо построение структурную электрическую схему для технологического процесса и продемонстрировать процесс работы.
Тема 14. Разработка Скада-систем.
Практическая работа 11. Разработка Скада-системы.
На основании предложенных вариантов необходимо разработать мнемо-схему для автоматизированного процесса.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Введение. Обзор современных автоматизированных систем и устройств.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
2.	Система теплоснабжения зданий различного назначения. Учет и регулировка теплоносителя.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
3.	Тепловые счетчики, их устройство и режимы работы.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
4.	Интерфейсы RS-232, RS-422 и RS-485.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
5.	Система погодного регулирования. Система управления газовыми	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.

	и твердотопливными котлами.	
6.	TPM32 контроллер для отопления и ГВС. СУНА-121 контроллер для групп насосов. Угрозы и аварийные ситуации.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
7.	Установки и устройства для поддержания микроклимата в помещениях/зданиях различного назначения. Модели угроз.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
8.	Системы охранно-пожарной сигнализации и пожаротушения. Организация диспетчерских пультов.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
9.	Системы видеонаблюдения. Проектирование сетей охранного телевидения. Виды оборудования. Защита данных.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
10.	Системы диспетчеризации. Их обустройство. Принципиальные схемы.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
11.	Среда проектирования Codesys. Алгоритмы работы контроллера ПЛК-150.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
12.	Принципы конфигурирования оборудования автоматизации.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
13.	Моделирование сетей и узлов систем автоматизации в различных средах. Имитационные модели.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.
14.	Разработка Скада-систем.	Чтение обязательной и дополнительной литературы, подготовка к практическим работам по подгруппам.

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение рекомендованной основной и дополнительной литературы.
3. Выполнение практической работы
4. Защита практической работы с объяснениями

Контроль за самостоятельной работой осуществляется при выполнении обучающимся практической работы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации – экзамен. Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса.

Вопросы к экзамену.

1. Виды технологических процессов и производств.
2. Критические производства. Аварийные и нештатные ситуации.
3. Узел учета тепловой энергии, его принцип работы и настройка.
4. Узел погодного регулирования и его принцип работы.
5. Нештатные ситуации, ошибки и отказы узлов учета тепловой энергии.
6. Угрозы вмешательства в работы УУТЭ и СПР.
7. Преобразователи интерфейсов, адресные множители и усилители.
8. Виды интерфейсов, протокол ModBus.
9. Основные угрозы на передатчики сотовой связи.
10. Системы управления газовыми и твердотопливными котлами. Организация защиты технологии и каналов связи.
11. Принцип работы контроллера ТРМ32 и его перевод на безаварийную ситуацию.
12. Принцип работы контроллера СУНА и алгоритмы безаварийной работы технологического оборудования.
13. Вентиляционные установки и их алгоритмы работы. Аварийные ситуации на примере технологического процесса.
14. Установки холодоснабжения, алгоритмы работы. Аварийные ситуации на примере технологического процесса.
15. Модели угроз для системы теплоснабжения производственного объекта.
16. Модели угроз для системы вентиляции административно-бытовых объектов.
17. Принципы работы охранно-пожарных систем сигнализации и пожаротушения. Нештатные ситуации.
18. Сблокированные пожарные системы с системами вентиляции и водоснабжения зданий. Основные информационные угрозы. Аварийные ситуации.
19. Автоматизация пожарных системы сигнализации и систем дымоудаления зданий различного назначения.
20. Системы видеонаблюдения мероприятия по защите оборудования и информации.
21. Виды оборудования видеонаблюдения и классификация. Адресные и аналоговые системы. Защита информации.
22. Способы подключения к камерам видеонаблюдения и обнаружение вторжений в адресную и не адресную сеть.
23. Основные этапы разработки мнемо-схем.
24. Способы увязки мнемо-схем с технологическим оборудованием.
25. Принципы имитационного моделирования технологического процесса.
26. Основные атаки на оборудование АСУТП.
27. Виды угроз на датчики автоматизированных систем.
28. Процесс перевода нагрузки на дублирующий контроллер. Этапы восстановления штатного рабочего режима.
29. Процесс организации аппаратной безопасности технологического процесса.
30. Участие систем видеонаблюдения в производственных процессах.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ПК-8 – способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы.	**Знать:** нормативно-техническую документацию; принцип работы оборудования автоматизированных систем; программное обеспечение для проектирования схем автоматизированных систем и узлов. **Уметь:** нормативно-техническую документацию; принцип работы оборудования автоматизированных систем; программное обеспечение для проектирования схем автоматизированных систем и узлов.	Практические работы по подгруппам, Билет кзамену	Компетенции сформированы при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. — Красноярск : Сибирский федеральный университет, 2019. — 206 с. — ISBN 978-5-7638-4008-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/100055.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей.

7.2. Дополнительная литература:

1. Рябцев, В. Г. Автоматизация технических систем специальных объектов : учебно-методическое пособие / В. Г. Рябцев. - Волгоград : ФГБОУ ВО Волгоградский ГАУ, 2019. - 84 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1087883 (дата обращения: 15.05.2020). – Режим доступа: по подписке.
2. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — Москва : РИОР

: ИНФРА-М, 2017. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380. - ISBN 978-5-369-01450-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/763644 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

7.3. Интернет-ресурсы

1. Научная электронная библиотека. URL: http://elibrary.ru/.
2. Электронные ресурсы ИБЦ ТюмГУ. URL: https://bmk.utmn.ru/ru/.

7.4 Современные профессиональные базы данных и информационные справочные системы

- Межвузовская электронная библиотека (МЭБ). - URL: https://icdlib.nspu.ru/
- Национальная электронная библиотека. - URL: https://rusneb.ru/
- Institute of Electrical and Electronics Engineers, Inc (IEEE). - URL: https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- Orbit Intelligence. - URL: https://www.orbit.com

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Лицензионное ПО:
  - Microsoft Imagine Academy (ранее Dreamspark): ОС семейства MS Windows (редакция Pro/Server);
  - Офисный пакет Microsoft Office 365 (лицензионное соглашение №2т/00509-20 от 12.05.2020);
  - Платформа для электронного обучения Microsoft Teams.

- Свободно распространяемое ПО:
  - Программное обеспечение виртуализации: VirtualBox (бесплатная лицензия доступна: https://www.virtualbox.org/wiki/Downloads).

9. **Технические средства и материально-техническое обеспечение дисциплины (модуля)**

Учебные аудитории для проведения лекций и практических занятий;

Лаборатории, оснащенные лабораторным оборудованием в соответствии с ФГОС ВО 3+ по данному направлению.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
“01” июня 2020 г.

АНАЛИЗ БОЛЬШИХ ДАННЫХ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Оленников А.А. Анализ больших данных. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность» специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Анализ больших данных [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Оленников А.А., 2020.

1. Пояснительная записка

Анализ больших данных позволяет ознакомиться с механизмами управления большими данными и основнями методами анализа больших данных.

Цель дисциплины «Анализ больших данных» - формирование компетенций, связанных с применением теоретических и практических знаний о больших данных, аналитике данных и инструментах по работе с большими данными при разработке ПО.

Задачи курса - изучение:

- знакомство с понятием Big Data и с технологиями управления данными;
- развить навыки применения технологий по работе с большими данными;
- изучить методы анализа данных;
- изучить построение тематических моделей и применение их для анализа данных;

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Дисциплина «Анализ больших данных» входит в блок Б1 Дисциплины (модули). Вариативная часть.

Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Математический анализ», «Языки программирования», «Введение в теорию вероятности и математическую статистику», «Технологии и методы программирования», «Администрирование операционных систем», «Информационные технологии», «Интернет вещей».

Дисциплина «Анализ больших данных» является одной из заключительных дисциплин 9 семестра. Способствует подготовке выпускной квалификационной работ.

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОПК-3 - способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации		Знает: основные понятия предметной области Big Data, принципы обработки больших данных в распределенных вычислительных системах, возможные сферы их приложений при решении практических задач. Умеет: использовать методы и технологии машинного обучения для решения прикладных задач, требующих обработку больших данных, выбирать технологии и методы анализа данных, а также адаптировать базовые методы к решению прикладных задач.

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		8 семестр
Общий объем зач. ед.	4	4
час.	144	144
Из них:		
Часы аудиторной работы (всего):	64	64
Лекции	32	32
Практические занятия	32	32
Лабораторные/практические занятия по подгруппам	0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	80	80
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет

3. Система оценивания

3.1. *Система текущего контроля*

Для текущего контроля применяется 100-балльная система оценивания. Баллы проставляются за посещение практических занятий и активную работу на них, а также за выполненные письменные и контрольные работы по каждой теме дисциплины. Результаты текущего контроля учитываются при промежуточной аттестации. Перевод баллов в зачет осуществляется по следующей шкале: от 61 до 100 баллов – «зачтено». Обучающиеся, не набравшие достаточного количества баллов, сдают зачет в период зачетной недели. Форма проведения зачета – собеседование по билетам. Собеседование включает один теоретический вопрос и одно практическое задание

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	**Наименование тем и/или разделов**	**Объем дисциплины (модуля), час.**				
		Всего	**Виды аудиторной работы** (академические часы)			**Иные виды контактной работы**
			Лекции	**Практические занятия**	**Лабораторные /практические занятия по подгруппам**	
1	2	3	4	5	6	7
1.	Введение	12	4	4	0	
2.	Предметная область Big Data	12	4	4	0	
3.	Принципы работы с	12	4	4	0	

	большими данными					
4.	Технологии работы с Big Data	18	6	6	0	
5.	Анализ данных и машинное обучение	18	4	4	0	
6.	Семантический анализ данных	18	4	4	0	
7.	Методы анализа больших данных	18	6	6	0	
	Итого (часов)	144	32	32	0	0

4.2. Содержание дисциплины (*модуля*) по темам

1. **Введение**

Основные цели и задачи изучения дисциплины. Структура курса. Организация лекционных и практических занятий. Самостоятельная работа. Формы контроля. Среды разработки.

2. **Предметная область Big Data**

Понятие Big Data. Основные этапы процесса анализа данных при решении прикладных задач. Анализ данных и машинное обучение Области применения технологий Big Data. Профессиональные направления в мире Big Data.

3. **Принципы работы с большими данными**

Основные принципы работы с большими данными. Набор признаков VVV (физический объём, скорость прироста данных и необходимости их быстрой обработки, возможность одновременно обрабатывать данные различных типов). Дополнительные признаки. Горизонтальная масштабируемость: количество вычислительных узлов, распределение данных, производительность. Отказоустойчивость: определение вероятности выхода машин из строя, учет ситуаций, превентивные меры. Локальность данных. Традиционные, централизованные, вертикальные модели хранения данных.

4. **Технологии работы с Big Data**

Средства массово-параллельной обработки неопределённо структурированных данных. Программные и технические решения по обработке сверхбольших массивов данных. Аппаратные средства. Модель распределённых параллельных вычислений в компьютерных кластерах (MapReduce), распределение элементарных заданий на узлы кластера, получение конечного результата. Нереляционные базы данных и хранилища (NoSQL). Выполнение распределённых программ, работающих на кластерах из узлов (Hadoop). Языки программирования для статистической обработки данных и работы с графикой.

5. **Анализ данных и машинное обучение**

Использование машинного обучения на больших данных на примере задачи классификации. Ассоциативные правила и анализ больших массивов данных на примере современных платформ.

6. **Семантический анализ данных**

Использование машинного обучения на больших данных на примере задачи классификации. Выявление и использование паттернов поведения в социальном графе с помощью Machine Learning. Особенности сбора, обработки и использования данных.

Компьютерная семантика. Формальные методы семантического анализа. Модели представления знаний в компьютерной семантике.

7. **Методы анализа больших данных**

Методы анализа, применимые к большим данным. Data Mining. Машинное обучение. Нейронные сети, сетевой анализ, оптимизация, генетические алгоритмы.

Планы практических занятий

Источники больших данных

– Доступные источники больших данных.
– Формирование наборов структурированных и неструктурированных данных для последующей обработки.
– Предварительная обработка данных.

Подготовка к реализации проекта по обработке больших данных

Проблематизация и обсуждение тем индивидуальных и коллективных проектов по работе с большими данными.
План работы над проектом

Информационные хранилища больших данных

Операции записи и чтения данных в HDFS.
Проектирование информационного обеспечения для решения задачи проекта.

Информационное хранилище: от SQL к NoSQL

Выбор СУБД и проектирование базы данных для решения задачи проекта.

Информационное хранилище: обоснование модели и выбора СУБД

Анализ ограничений SQL модели базы данных для решения задачи проекта.

Информационное хранилище: обоснование модели и выбора NoSQL СУБД

Анализ преимуществ NoSQL модели базы данных для решения задачи проекта.
Обоснование выбора СУБД.

Информационное хранилище: обоснование модели и выбора NewSQL СУБД

Анализ преимуществ NewSQL модели базы данных для решения задачи проекта.
Обоснование выбора СУБД.

Модель обработки данных

Анализ особенностей обработки данных для решения задачи проекта. Обоснование выбора модели обработки (паттернов программирования).

Компоненты и алгоритм работы HDFS

Анализ особенностей распределенного хранения данных для решения задачи проекта.
Программная реализация функционала для работы с HDFS.

Практическое задание 1

Отбор данных для решения задач машинного обучения - доступные источники данных.
Формирование наборов структурированных и неструктурированных данных для обучения модели.
Предварительная обработка данных.

Практическое задание 2

Обсуждение этапов процесса по построению моделей машинного обучения.
Сравнение обработки больших данных и «стандартных» сценариев работы с объемами данных.

Практическое задание 3

Контроль усвоения материала, разбиравшегося на лекциях.
Разбор решений практических задач, определение набора признаков VVV.
Исследование традиционных, централизованных, вертикальных моделей хранения данных.
Самостоятельное выполнение практических заданий.
Защита выполненных заданий.

Практическое задание 4

Контроль усвоения материала, разбиравшегося на лекциях.

Разбор решений практических задач с применением модели распределённых параллельных вычислений в компьютерных кластерах.

Разбор решений практических задач с применением распределённых программ, работающих на кластерах из узлов

Самостоятельное выполнение практических заданий.

Защита выполненных заданий.

Практическое задание 5

Знакомство и приобретение практических навыков работы с такими ресурсами как WordNet, FrameNet.

Знакомство с тезаурусами для русского языка.

Выявление и использование паттернов поведения в графе с помощью Machine Learning

Оценка точности решения.

Практическое задание 6

Контроль усвоения материала, разбиравшегося на лекциях.

Разбор решений практических задач с применением методов и техник анализа, применимых к большим данным.

Проверка гипотез о виде предполагаемого распределения.

Исследование взаимосвязей категориальных признаков.

Самостоятельное выполнение практических заданий.

Защита выполненных заданий.

Практическое задание 7

Контроль усвоения материала, разбиравшегося на лекциях.

Знакомство с редакторами и свободными программами для построения сложных диаграмм.

Анализ и исследование использование программных модулей.

Самостоятельное выполнение практических заданий.

Защита выполненных заданий.

Практическое задание 8

Контроль усвоения материала, разбиравшегося на лекциях.

Особенности обработки массивов данных в режиме реального времени.

Использование технологий Big Data при решении прикладных задач.

Самостоятельное выполнение практических заданий.

Защита выполненных заданий.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Введение в дисциплину	Проработка лекций. Чтение обязательной и дополнительной литературы
2.	Предметная область DataScience	Проработка лекций. Чтение обязательной и дополнительной литературы. Подготовка к практическим занятиям
3.	Принципы работы с	Проработка лекций. Чтение обязательной и

	большими данными	дополнительной литературы. Подготовка к практическим занятиям
4.	Технологии и тенденции работы с Big Data	Проработка лекций. Чтение обязательной и дополнительной литературы. Подготовка к практическим занятиям
5.	Big Data: семантический анализ данных и машинное обучение	Проработка лекций. Чтение обязательной и дополнительной литературы. Подготовка к практическим занятиям
6.	Методы и техники анализа больших данных	Проработка лекций. Чтение обязательной и дополнительной литературы. Подготовка к практическим занятиям
7.	Визуализация аналитических данных	Проработка лекций. Чтение обязательной и дополнительной литературы. Подготовка к практическим занятиям
8.	Большие данные в промышленности	Проработка лекций. Чтение обязательной и дополнительной литературы. Подготовка к практическим занятиям
9.	Аппаратно-программные комплексы, предназначенные для обработки больших данных	Проработка лекций. Чтение обязательной и дополнительной литературы. Подготовка к практическим занятиям
10.	Рынок Big data в России	Проработка лекций. Чтение обязательной и дополнительной литературы. Подготовка к практическим занятиям

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение основной и дополнительной литературы.
3. Разбор примеров практических занятий.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации – зачет.
Зачет проводится в виде собеседования по вопросам билета.
Пример задания: билет содержит 1 теоретический вопрос из списка примерных вопросов и 1 практическое задание, связанное с содержанием теоретического вопроса.

Теоретическая часть:
Средства массово-параллельной обработки неопределённо структурированных данных.

Практическая часть
Для заданного набора данных определить набор признаков VVV.

Вопросы к зачету:

1. Понятие больших данных (Big Data, BD). Модель 3-V больших данных. Основные характеристики модели.
2. Требования к системам обработки в контексте характеристик BD. Модель 3-V для оценки производительности экосистемы.
3. Экосистемы BD и машинное обучение. Понятие вертикального и горизонтального масштабирования системы обработки данных.
4. Информационное хранилище: место в экосистеме обработки BD. Распределенные файловые системы. Примеры. Hadoop Distributed File System (HDFS) как основа различных систем обработки BD.
5. Понятие Not only SQL. Принципы ACID. Примеры реализации в системах обработки данных.
6. Теорема Брюера, или принципы CAP. Следствия: модели CA, AP, CP.
7. Принципы BASE для NoSQL. Примеры реализации в системах обработки данных. Преимущества и ограничения модели.
8. Модели данных NoSQL. Column-Oriented - столбцовые БД. Соответствие моделей принципам ACID, BASE. Примеры СУБД, реализующих модель данных.
9. Модели данных NoSQL. .Key-Value - хранилища ключ-значение. Соответствие моделей принципам ACID, BASE. Примеры СУБД, реализующих модель данных.
10. Модели данных NoSQL. Графовые БД. Соответствие моделей принципам ACID, BASE. Примеры СУБД, реализующих модель данных.
11. Модели данных NoSQL. Document-Oriented - хранилища документов. Соответствие моделей принципам ACID, BASE. Примеры СУБД, реализующих модель данных.
12. Парадигма MapReduce. Описание вычислительного процесса. Преимущества и ограничения модели MapReduce. Примеры реализации на различных языках программирования.
13. Экосистема Apache Hadoop. Базовые компоненты Hadoop: обзор функционала.
14. Hadoop Distributed File System (HDFS). Компоненты и алгоритм работы HDFS. Read/Write запросы HDFS. Примеры реализации на различных языках программирования.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения	Оценочные материалы	Критерии оценивания
1.	ОПК-3 - способность понимать значение информации в развитии современного общества, применять достижения	Знает и умеет использовать методы и технологии машинного обучения для решения прикладных задач, требующих обработку больших данных, выбирать новые технологии и методы анализа данных, а	Собеседование (вопросы по темам заданий)	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине

	информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации	также адаптировать базовые методы к решению прикладных задач.		понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература:

1. Чубукова, И. А. Data Mining : учебное пособие / И. А. Чубукова. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 469 c. — ISBN 978-5-4497-0289-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89404.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

7.2 Дополнительная литература:

1. Методы и модели исследования сложных систем и обработки больших данных : монография / И. Ю. Парамонов, В. А. Смагин, Н. Е. Косых, А. Д. Хомоненко ; под редакцией В. А. Смагинаи А. Д. Хомоненко. — Санкт-Петербург : Лань, 2020. — 236 с. — ISBN 978-5-8114-4006-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126938 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.
2. Щербакова, Ю. В. Теория вероятностей и математическая статистика : учебное пособие / Ю. В. Щербакова. — 2-е изд. — Саратов : Научная книга, 2019. — 159 c. — ISBN 978-5-9758-1786-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/81056.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

7.3 Интернет-ресурсы:

1. вузовские электронно-библиотечные системы учебной литературы.
2. http://www.infosecurity. Report.ru (портал по информационной безопасности).
3. база научно-технической информации ВИНИТИ РАН.

7.4 Современные профессиональные базы данных и информационные справочные системы:

1. Базы данных научно-технической информации, научных трудов, статей, материалов, доступных в Тюменском государственном университете https://www.utmn.ru/upload/medialibrary/fc5/Perechen-podpisnykh-litsenzionnykh-baz-dannykh-i-baz-dannykh-dostupnykh-v-ramkakh-natsionalnoy-podpiski.doc (дата обращения: 15.05.2020).

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Для организации самостоятельной работы студентов необходим компьютерный класс с пакетом прикладных программ, в том числе с установленной средой разработки на языке C#, C++, Pascal, Java, VirtualBox.
- платформа для электронного обучения Microsoft Teams.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения лекций и практических занятий;

Лаборатории, оснащенные лабораторным оборудованием в соответствии с ФГОС ВО 3+ по данному направлению.

Для организации самостоятельной работы студентов необходим компьютерный класс с пакетом прикладных программ, в том числе с установленной средой разработки на языке C#, C++, Pascal, Java, VirtualBox.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
“01” июня 2020 г.

БЕЗОПАСНОСТЬ СЕТЕЙ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ МАШИН
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Захаров А.А. Безопасность сетей электронно-вычислительных машин. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Безопасность сетей электронно-вычислительных машин [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Захаров А.А., 2020.

1. Пояснительная записка

Дисциплина «Безопасность сетей электронно-вычислительных машин» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Цель дисциплины «Безопасность сетей электронно-вычислительных машин» - является изложение основополагающих принципов разработки сетевого программного обеспечения в различных средах с использованием различных информационных технологий при решении разнообразных прикладных задач.

Задачи курса - изучение:

- основных принципов разработки сетевых протоколов;
- основных принципов анализа сетевых протоколов;
- принципов разработки сетевых программ и выбора технологии и протокола передачи данных.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Организация электронно-вычислительных машин и вычислительных систем», «Структуры и алгоритмы компьютерной обработки данных», «Языки программирования».

Дисциплина «Безопасность сетей электронно вычислительных машин» способствует освоению следующих дисциплин: «Разработка и защита web приложений», «Безопасность операционных систем», «Безопасность систем баз данных».

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-8 - способность к самоорганизации и самообразованию		Знает: содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности. Умеет: самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности; планировать цели и устанавливать приоритеты при выборе способов принятия решений с учетом условий, средств, личностных возможностей и временной перспективы достижения.
ПК-5 - способность участвовать в разработке и		Знает: принципы функционирования протоколов

конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		FTP, HTTP, SMTP и POP3, стандартные команды протоколов. Умеет: производить основные действия с протоколами FTP, HTTP, SMTP или POP3 программно.
ПК-10 - способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		Знает: назначение, преимущества и недостатки протоколов FTP, HTTP, SMTP и POP3. Умеет: производить проверку безопасности реализации протоколов FTP, HTTP, SMTP и POP3.
ПК-18 - способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		Знает: Basic, Digest, NTLM и авторизацию с помощью форм. Умеет: настраивать Basic, Digest, NTLM и авторизацию с помощью форм.

* не предусмотрено

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		5 семестр
Общий объем зач. ед.	4	4
час.	144	144
Из них:		

Часы аудиторной работы (всего):	64	64
Лекции	32	32
Практические занятия	32	32
Лабораторные/практические занятия по подгруппам	0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	80	80
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		экзамен

3. Система оценивания

3.1. Для текущего контроля применяется 100-балльная система оценивания. Баллы проставляются за выполненные лабораторные работы по каждой теме дисциплины. Результаты текущего контроля учитываются при промежуточной аттестации. Перевод баллов в оценки осуществляется по следующей шкале: от 91 до 100 баллов – «отлично»; от 76 до 90 баллов – «хорошо»; от 61 до 75 баллов – «удовлетворительно». Обучающиеся, не набравшие достаточного количества баллов для оценки, сдают экзамен в период экзаменационной сессии. К экзамену допускаются студенты, набравшие за семестр 35 баллов. Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должен быть сделан ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Ответ может содержать небольшие недочеты, наличие примеров необязательно. Для получения оценки «хорошо» студентом должно быть выполнено практическое задание и сделан ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Ответ может содержать небольшие недочеты, наличие примеров обязательно. Для получения оценки «отлично» студент должен выполнить практическое задание и сделать ответ на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	**Наименование тем и/или разделов**	**Объем дисциплины (модуля), час.**				
		Всего	**Виды аудиторной работы** (академические часы)			**Иные виды контактной работы**
			Лекции	**Практические занятия**	**Лабораторные /практические занятия по подгруппам**	

1	2	3	4	5	6	7
1.	Основные понятия.	8	4	0	4	0
2.	Протокол HTTP.	8	4	0	4	0
3.	Протокол FTP.	8	4	0	4	0
4.	Протокол POP3.	8	4	0	4	0
5.	Протокол SMTP.	8	4	0	4	0
6.	Уязвимости сетевых протоколов.	4	2	0	2	0
7.	Обзор современных сетевых протоколов.	8	4	0	4	0
8.	Разработка сетевых приложений на базе протокола TCP.	4	2	0	2	0
9.	Анонимные и именованные каналы связи.	8	4	0	4	0
	Итого (часов)	144	32		32	2

4.2. Содержание дисциплины (*модуля*) по темам

Модуль 1

1. Основные понятия.

Протоколы TCP и UDP. Сетевые протоколы уровня приложения. Понятие стандарта на протокол. Стандарты RFC и IETF.

2. Протокол HTTP.

История протокола. Версии протокола. Структура запроса.
Структура ответа. Поля. Коды ответов и их значения. Аутентификация в протоколе HTTP.

3. Протокол FTP.

История протокола. Версии протокола. Команды протокола.
Структура ответа. Коды ответов и их значения. Аутентификация.

Модуль 2

4. Протокол POP3.

История протокола. Команды протокола. Коды ответов и их значения.
Аутентификация.

5. Протокол SMTP.

История протокола. Команды протокола. Коды ответов и их значения.

6. Уязвимости сетевых протоколов.

Уязвимости протокола HTTP. Уязвимости протокола FTP. Уязвимости протокола POP3. Уязвимости протокола SMTP.

Модуль 3

7. Обзор современных сетевых протоколов.

Обзор наиболее существенных современных сетевых протоколов.

8. Разработка сетевых приложений на базе протокола TCP.

Подходы к разработке сетевых приложений. Сетевая библиотека WinSock. Разработка сетевого приложения на базе оконных сообщений. Разработка сетевого приложения на базе событий. Разработка сетевого приложения в блокирующем режиме. Разработка сетевого приложения в режиме асинхронного завершения операций.

9. Анонимные и именованные каналы связи.
Понятие канала. Возможности и назначение канала. Анонимные и именованные каналы связи. Передача информации через канал.

Планы семинарских занятий.
Не предусмотрены.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Основные понятия.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторных работ, подготовка к собеседованию.
2.	Протокол HTTP.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторных работ, подготовка к собеседованию.
3.	Протокол FTP.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторных работ, подготовка к собеседованию.
4.	Протокол POP3.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторных работ, подготовка к собеседованию.
5.	Протокол SMTP.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторных работ, подготовка к собеседованию.
6.	Уязвимости сетевых протоколов.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторных работ, подготовка к собеседованию.
7.	Обзор современных сетевых протоколов.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторных работ, подготовка к собеседованию.
8.	Разработка сетевых приложений на базе протокола TCP.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторных работ, подготовка к собеседованию.
9.	Анонимные и именованные каналы связи.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторных работ, подготовка к собеседованию.

Порядок выполнения каждого вида самостоятельной работы:

1. Конспектирование материала на лекционных занятиях.

2. Работа с учебной литературой.
3. Выполнение лабораторных работ, подготовка к собеседованию.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения экзамена – Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса.

Вопросы к экзамену

1 В чем состоит отличие протоколов TCP и UDP. Каковы последствия этого различия для передачи информации. Объясните на примерах.
2 Что такое стандартизированный протокол? Как происходит выработка стандарта на протокол?
3 Какие вы знаете протоколы, описанные в RFC. Охарактеризуйте их (Назначение, принцип работы).
4 Опишите назначение и принцип работы протокола HTTP. Ответ сопроводите примерами.
5 Опишите основные отличия протокола HTTP/1.0 от протокола HTTP/1.1.
6 Опишите структуру HTTP запроса. Какие методы запроса вы знаете. Опишите их. Опишите способы передачи информации от клиента на сервер.
7 Опишите структуру HTTP ответа. Опишите стандартные ответы сервера и их значение.
8 Какие способы определения конца HTTP сообщения вам известны. Опишите их.
9 Какие уязвимости HTTP протокола вам известны. Опишите их и расскажите, как их можно избежать.
10 Опишите принцип работы протокола FTP. Опишите основные команды и ответы на них.
11 Опишите основные уязвимости протокола FTP. Объясните, как скопировать файл с одного FTP сервера на другой минуя клиента.
12 Опишите принцип работы протокола POP3. Опишите основные команды и ответы на них.
13 Опишите принцип работы протокола SMTP. Опишите основные команды и ответы на них.
14 Опишите принцип функционирования сетевого приложения на базе оконных сообщений.
15 Опишите принцип функционирования сетевого приложения на базе событий Windows.
16 Опишите принцип функционирования сетевого приложения в блокирующем режиме.
17 Опишите принцип функционирования сетевого приложения в режиме асинхронного завершения.
18 Опишите процесс взаимодействия приложений через именованные каналы.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОК-8 - способность к самоорганизации и самообразованию	Знает: содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности. Умеет: самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности; планировать цели и устанавливать приоритеты при выборе способов принятия решений с учетом условий, средств, личностных возможностей и временной перспективы достижения.	Лабораторная работа, экзаменационный билет	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-5 - способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты	Знает: принципы функционирования протоколов FTP, HTTP, SMTP и POP3, стандартные команды протоколов. Умеет: производить основные действия с протоколами FTP, HTTP, SMTP или POP3 программно.	Лабораторная работа, экзаменационный билет	

	информации			
3.	ПК-10 - способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает: назначение, преимущества и недостатки протоколов FTP, HTTP, SMTP и POP3. Умеет: производить проверку безопасности реализации протоколов FTP, HTTP, SMTP и POP3.	Лабораторная работа, экзаменационный билет	
4.	ПК-18 - способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства	Знает: Basic, Digest, NTLM и авторизацию с помощью форм. Умеет: настраивать Basic, Digest, NTLM и авторизацию с помощью форм.	Лабораторная работа, экзаменационный билет	

	криптографической защиты информации			

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Сети связи и системы коммутации: Учебное пособие / Паринов А.В., Ролдугин С.В., Мельник В.А. - Воронеж:Научная книга, 2016. - 178 с. ISBN 978-5-4446-0906-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/923309 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

7.2. Дополнительная литература:

1. Архитектура ЭВМ и систем : учебное пособие / Ю. Ю. Громов, О. Г. Иванова, М. Ю. Серегин [и др.]. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2012. — 200 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/64069.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

2. Компьютерные сети : учебно-методический комплекс / составители О. С. Ахметова, А. Опабекова, А. М. Сатымбеков. — Алматы : Нур-Принт, 2012. — 295 с. — ISBN 9965-756-19-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/67067.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

7.3. Интернет-ресурсы

1. вузовские электронно-библиотечные системы учебной литературы.
2. база научно-технической информации ВИНИТИ РАН
3. доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru
4. http://www.ietf.org/rfc.html [On-line] - документы IETF – инженерного совета Интернета.
5. http://msdn.microsoft.com

7.4 Современные профессиональные базы данных и информационные справочные системы:

https://www.utmn.ru/obrazovanie/normativnye-dokumenty/akkteditatsiya/dokumenty-tyumgu/.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Лицензионное ПО:**
- **ПО, находящееся в свободном доступе:**
- Visual Studio;
- пакет Microsoft Office Professional 2013;
- Borland Delphi 7 или выше;
- Microsoft SQL Server 2008 или выше;
- Службы активного каталога;
- IIS7.0 или выше.
- среда для электронного обучения MS Teams.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

- компьютерный класс;
- мультимедийная лекционная аудитория с доступом к сети интранет и интернет и установленным в ней ПО.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
“01” июня 2020 г.

БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Нестерова О.А Безопасность систем баз данных. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Безопасность систем баз данных [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Нестерова О.А, 2020.

1. Пояснительная записка

Безопасность систем баз данных обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Цель дисциплины «Безопасность систем баз данных» - формирование у студентов совокупности профессиональных качеств, обеспечивающих решение проблем, связанных с использованием и проектированием баз данных под управлением современных систем управления базами данных (СУБД), а также связанных с обеспечением безопасности информации в автоматизированных информационных системах (АИС), основу которых составляют базы данных (БД) навыкам работы со встроенными в системы управления базами данных (СУБД) средствами защиты.

Задачи курса - изучение:

• обучить студентов принципам работы современных систем управления базами данных;

• привить студентам навыки проектирования и реализации баз данных;

• приобретение системного подхода к проблеме защиты информации в СУБД;

• изучение моделей и механизмов защиты в СУБД;

• приобретение практических навыков организации защиты БД.

• обучить студентов проводить обоснование и выбор рационального решения по защите систем управления баз данных с учетом заданных требований;

• обучить студентов формализовать поставленную задачу по обеспечению защиты БД;

• обучить студентов применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;

• привить студентам навыки разработки нормативных и организационнораспорядительных документов, регламентирующих работу по защите информации в СУБД

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Блок 1.Дисциплины (модули). Б1.Б.26. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Технологии и методы программирования», «История создания, хранения, передачи и защиты информации»

Дисциплина «Безопасность систем баз данных» способствует освоению следующих дисциплин: «Анализ больших данных», «Управление информационной безопасностью»

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-8 - способность к самоорганизации и самообразованию		***знать:*** - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; ***уметь:*** - самостоятельно строить процесс овладения информацией, отобранной и структурированной для

		выполнения профессиональной деятельности;
ПК-10 - способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты,		Знать: основные средства и способы обеспечения информационной безопасности, предоставляемые системами управления базами данных; принципы построения систем защиты информации; Уметь: использовать средства защиты, предоставляемые системами управления базами данных; проводить обоснование и выбор рационального решения по защите систем управления баз данных с учетом заданных требований;
ПК-18 - способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		Знать: сущность и понятие информации, информационной безопасности и характеристику ее составляющих; средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; современные критерии и стандарты для анализа безопасности информационных систем на базе СУБД; Уметь: анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты для проектирования, разработки и оценивания защищенности компьютерной системы;

* не предусмотрено

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		7 семестр
Общий объем зач. ед.	4	4
час.	144	144
Из них:		
Часы аудиторной работы (всего):	64	64
Лекции	32	32

Практические занятия	32	32
Лабораторные/практические занятия по подгруппам	0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	53	53
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		экзамен

3. Система оценивания

3.1. Для текущего контроля применяется 100-балльная система оценивания. Баллы проставляются за посещение практических занятий и активную работу на них, а также за выполненные лабораторные работы по каждой теме дисциплины. Результаты текущего контроля учитываются при промежуточной аттестации. Перевод баллов осуществляется по следующей шкале: более 91 балла – «отлично»; от 76 до 91 – «хорошо»; от 61 до 75 – «удовлетворительно»; менее 61 балла – «неудовлетворительно». Обучающиеся, не набравшие достаточного количества баллов для оценки, сдают экзамен в период сессии. Форма проведения экзамена – контрольная работа. Продолжительность выполнения - астрономический час.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	**Наименование тем и/или разделов**	**Объем дисциплины (модуля), час.**				
		Всего	**Виды аудиторной работы** (академические часы)			**Иные виды контактной работы**
			Лекции	**Практические занятия**	**Лабораторные /практические занятия по подгруппам**	
1	2	3	4	5	6	7
Модуль 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ БЕЗОПАСНОСТИ В БД						
1.	Безопасность БД, угрозы, защита	10	2	2	0	0
2.	Критерии защищенности БД	10	2	2	0	0
3.	Модели безопасности в СУБД	10	4	4	0	0
Модуль 2. СРЕДСТВА И МЕТОДЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ БД						
4.	Средства идентификации и аутентификации	20	4	4	0	0
5.	Средства управления доступом	20	4	4	0	0
6.	Целостность БД и способы ее обеспечения	20	4	4	0	0

Модуль 3. СРЕДСТВА И МЕТОДЫ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ И ДОСТУПНОСТИ БД						
7.	Классификация угроз конфиденциальности СУБД	15	4	4	0	0
8.	Аудит и подотчетность	15	4	4	0	0
9.	Транзакции и блокировки	24	4	4	0	0
	Итого (часов)	144	32	32	0	2

4.2. Содержание дисциплины (*модуля*) по темам

Модуль 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ БЕЗОПАСНОСТИ В БД

Тема 1. Безопасность БД, угрозы, защита.

Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные. Требования безопасности БД. История развития, назначение и роль баз данных. Модели данных. Математические основы построения реляционных СУБД.

Тема 2. Критерии защищенности БД.

Критерии оценки надежных компьютерных систем (TCSEC). Понятие политики безопасности. Совместное применение различных политик безопасности в рамках единой модели. Интерпретация TCSEC для надежных СУБД (TDI). Оценка надежности СУБД как компоненты вычислительной системы.

Тема 3. Модели безопасности в СУБД.

Дискреционная (избирательная) и мандатная (полномочная) модели безопасности. Классификация моделей. Аспекты исследования моделей безопасности. Особенности применения моделей безопасности в СУБД.

Модуль 2. СРЕДСТВА И МЕТОДЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ БД

Тема 4. Средства идентификации и аутентификации.

Общие сведения. Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС.

Тема 5. Средства управления доступом.

Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Виды привилегий: привилегии безопасности и доступа. Использование ролей и привилегий пользователей. Соотношение прав доступа, определяемых ОС и СУБД. Использование представлений для обеспечения конфиденциальности информации в СУБД. Средства реализации мандатной политики безопасности в СУБД.

Тема 6. Целостность БД и способы ее обеспечения.

Основные виды и причины возникновения угроз целостности. Способы противодействия. Цели использования триггеров. Способы задания, моменты выполнения. Декларативная и процедурная ссылочные целостности. Внешний ключ. Способы поддержания ссылочной целостности.

Модуль 3. СРЕДСТВА И МЕТОДЫ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ И ДОСТУПНОСТИ БД

Тема 7. Классификация угроз конфиденциальности СУБД.

Причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД, частичное разглашение. Получение несанкционированного доступа к конфиденциальной информации путем логических

выводов. Методы противодействия. Особенности применения криптографических методов. ***Тема 8. Аудит и подотчетность.***

Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.

Тема 9. Транзакции и блокировки.

Транзакции как средство изолированности пользователей. Сериализация транзакций. Методы сериализации транзакций. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. Тупиковые ситуации, их распознавание и разрушение.

Примерные темы лабораторных занятий

Тема 1. Основы построения и эксплуатации баз данных.

Построение реляционных СУБД. Эксплуатация баз данных. Автоматизированное проектирование баз данных.

Тема 2. Безопасность БД, угрозы, защита.

Угрозы безопасности БД: общие и специфичные. Требования безопасности БД. История развития, назначение и роль баз данных. Модели данных. Математические основы построения реляционных СУБД.

Тема 3. Модели безопасности в СУБД.

Дискреционная (избирательная) и мандатная (полномочная) модели безопасности. Классификация моделей. Исследование моделей безопасности. Применение моделей безопасности в СУБД.

Тема 4. Средства идентификации и аутентификации.

Применение средств идентификации и аутентификации, встроенных в СУБД и в ОС.

Тема 5. Средства управления доступом

Использование ролей и привилегий пользователей. Использование представлений для обеспечения конфиденциальности информации в СУБД.

Использование средств реализации политик безопасности в СУБД.

Тема 6. Целостность БД и способы ее обеспечения

Способы обеспечения целостности БД. Использование триггеров. Применение декларативной и процедурной ссылочные целостности. Способы поддержания ссылочной целостности. Резервное копирование и восстановление базы данных.

Тема 7. Классификация угроз конфиденциальности СУБД

Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы противодействия. Применение криптографических методов.

Тема 8. Аудит и подотчетность

Подотчетность действий пользователя и аудит связанных с безопасностью событий.

Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.

Тема 9. Транзакции и блокировки.

Применение транзакций как средства изолированности пользователей. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. Тупиковые ситуации, их распознавание и разрушение.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Безопасность БД, угрозы, защита	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы
2.	Критерии защищенности БД	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы
3.	Модели безопасности в СУБД	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы
4.	Средства идентификации и аутентификации	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы
5.	Средства управления доступом	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы
6.	Целостность БД и способы ее обеспечения	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы
7.	Классификация угроз конфиденциальности СУБД	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы
8.	Аудит и подотчетность	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы
9.	Транзакции и блокировки	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение рекомендованной основной и дополнительной литературы.
3. Выполнение лабораторной работы
4. Защита лабораторной работы с объяснениями

Контроль за самостоятельной работой осуществляется при выполнении обучающимся лабораторной работы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения – экзамен.

Вопросы к зачету

1. Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные.
2. Понятие политики безопасности. Сущность политики безопасности.

3. Цели формализации политики безопасности.
4. Принципы построения защищенных систем.
5. Дискреционные модели безопасности СУБД.
6. Реализация ролевой модели политики безопасности в СУБД Oracle.
7. Реализация ролевой модели политики безопасности в СУБД MS SQL Server.
8. Мандатная модель политики безопасности.
9. БД с многоуровневой секретностью (MLS).
10. Многозначность. Реализация модели MLS.
11. Авторизация меток пользователя. Специальные привилегии доступа.
12. Меточные функции. Опции ограничения.
13. Метаданные и словарь данных. Назначение словаря данных.
14. Доступ к словарю данных.
15. Состав словаря данных. Представления словаря.
16. Понятие транзакции. Фиксация транзакции.
17. Прокрутки вперед и назад. Контрольная точка. Откат.
18. Транзакции как средство изолированности пользователей.
19. Сериализация транзакций.
20. Блокировки. Режимы блокирования.
21. Правила согласования блокировок.
22. Двухфазный протокол синхронизационных блокировок.
23. Взаимоблокировки, их распознавание и разрушение.
24. Целостность кода приложения. SQL-инъекции.
25. Динамическое выполнение кода SQL и PL/SQL.
26. Категории атак SQL-инъекцией. Методы SQL-инъекций.
27. Противодействие атакам типа SQL-инъекции.
28. Подотчетность действий пользователя и аудит связанных с безопасностью событий.
29. Регистрация действий пользователя.
30. Управление набором регистрируемых событий.
31. Анализ регистрационной информации

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОК-8 - способность к самоорганизации и самообразованию	знать: - содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности; уметь: - самостоятельно строить	Собеседование, лабораторные работы, экзаменационные билеты	Компетенции сформированы при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и

		процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;		правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-10 - способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты,	Знать: основные средства и способы обеспечения информационной безопасности, предоставляемые системами управления базами данных; принципы построения систем защиты информации; Уметь: использовать средства защиты, предоставляемые системами управления базами данных; проводить обоснование и выбор рационального решения по защите систем управления баз данных с учетом заданных требований;	Собеседование, лабораторные работы, экзаменационные билеты	
3.	ПК-18 - способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства	Знать: сущность и понятие информации, информационной безопасности и характеристику ее составляющих; средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; современные критерии и стандарты для анализа безопасности информационных систем на базе СУБД; Уметь: анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты для проектирования, разработки	Собеседование, лабораторные работы, экзаменационные билеты	

	криптографической защиты информации	и оценивания защищенности компьютерной системы;		

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Мартишин, С. А. Базы данных. Практическое применение СУБД SQL и NoSQL-типа для проектирования информационных систем: учебное пособие / С.А. Мартишин, В.Л. Симонов, М.В. Храпченко. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2016. — 368 с. — (Высшее образование). - ISBN 978-5-8199-0660-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/556449 (дата обращения: 15.05.2020). – Режим доступа: по подписке

7.2. Дополнительная литература:

1. Дадян, Э. Г. Методы, модели, средства хранения и обработки данных : учебник / Э.Г. Дадян, Ю.А. Зеленков. — Москва : Вузовский учебник : ИНФРА-М, 2017. — 168 с. - ISBN 978-5-9558-0490-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/543943 (дата обращения: 15.05.2020). – Режим доступа: по подписке.
2. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2017. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380. - ISBN 978-5-369-01450-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/763644 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

7.3. Интернет-ресурсы

1. вузовские электронно-библиотечные системы учебной литературы.
2. http://www.infosecurity. Report.ru (портал по информационной безопасности).
3. база научно-технической информации ВИНИТИ РАН.
4. среды разработки на языках C#, C++, Delphi.
5. Порталы разработчиков систем управления базами данных: MS SQL Server, InterBase/FireBird, MySQL, Oracle, SQL Postgre.

7.4 Современные профессиональные базы данных и информационные справочные системы

Базы данных научно-технической информации, научных трудов, статей, материалов, доступных в Тюменском государственном университете https://www.utmn.ru/upload/medialibrary/fc5/Perechen-podpisnykh-litsenzionnykh-baz-dannykh-i-baz-dannykh-dostupnykh-v-ramkakh-natsionalnoy-podpiski.doc (дата обращения: 15.05.2020).

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Для организации самостоятельной работы студентов необходим компьютерный класс с пакетом прикладных программ, в том числе с установленной средой разработки на языке C#, C++, Pascal, Java, с системами управления базами данных: MS SQL Server 2017, Oracle 10g – Oracle 11g, со средством моделирования MS Office Visio.
- платформа для электронного обучения Microsoft Teams.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения лекций и практических занятий;

Лаборатории, оснащенные лабораторным оборудованием в соответствии с ФГОС ВО 3+ по данному направлению.

Для организации самостоятельной работы студентов необходим компьютерный класс с пакетом прикладных программ, в том числе с установленной средой разработки на языке C#, C++, Pascal, Java, с системами управления базами данных: MS SQL Server, InterBase/FireBird, MySQL, со средством моделирования MS Office Visio.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
“01” июня 2020 г.

ВЫСШАЯ МАТЕМАТИКА
Рабочая программа
для обучающихся по специальности 10.05.01 Компьютерная безопасность
Специализация: Безопасность распределенных компьютерных систем
форма обучения - очная

Иванов Д. И. Высшая математика Рабочая программа для обучающихся по специальности 10.05.01 Компьютерная безопасность, специализация: Безопасность распределенных компьютерных систем, форма обучения – очная. Тюмень, 2020.

Рабочая программа дисциплины Высшая математика опубликована на сайте ТюмГУ: Высшая математика [электронный ресурс] / Режим доступа: https://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Иванов Д. И., 2020.

1. Пояснительная записка

Цели и задачи дисциплины:

Целями преподавания дисциплины являются:

- формирование и развитие навыков математического мышления, навыков использования математических методов и основ математического моделирования, математической культуры у обучающихся;
- обеспечение высокого уровня фундаментальной математической подготовки студентов, необходимого для дальнейшего обучения и успешного усвоения специальных дисциплин;
- приобретение навыков самостоятельного изучения отдельных тем дисциплины и решения типовых задач;
- усвоение полученных знаний студентами, а также формирование у них мотивации к самообразованию за счет активизации их познавательной деятельности.

Задачи изучения дисциплины:

- формирование у студентов базовых знаний об основных математических объектах и структурах,
- освоение методов работы с указанными объектами;
- изучение алгоритмов решения типовых задач;
- обзор возможностей применения изученных моделей и методов к решению различных задач.

1.1. Место дисциплины в структуре образовательной программы

Дисциплина относится к блоку Б1 дисциплин обязательной части.

Для успешного освоения дисциплины студенты должны обладать знаниями и умениями, полученными при изучении школьных курсов «Алгебра и начала анализа» и «Геометрия».

На основе приобретенных знаний формируются умения применять математические методы при решении профессиональных задач повышенной сложности, владеть методами построения математической модели профессиональных задач и содержательной интерпретации полученных результатов.

Знание основ высшей математики может существенно помочь в научно-исследовательской работе

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины

Код и наименование компетенции (из ФГОС ВО)	Код и наименование части компетенции (при наличии паспорта компетенций)	Компонент (знаниевый/функциональный)
Способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов. (ОПК-2)	ОПК-2	Знает основные понятия, теоремы и методы алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, использующихся при изучении общетеоретических и специальных дисциплин учебного цикла; Уметет использовать знания фундаментальных основ, подходы и методы математики при решении прикладных задач; пользоваться источниками для самостоятельного изучения специальной литературы;

1.3. Перечень планируемых результатов освоения дисциплины (модуля):

В результате изучения дисциплины студент должен:

знать:

основные понятия, теоремы и методы алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, использующихся при изучении общетеоретических и специальных дисциплин учебного цикла;

уметь:

использовать знания фундаментальных основ, подходы и методы математики при решении прикладных задач;

пользоваться источниками для самостоятельного изучения специальной литературы;

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Часов в семестре**			
			2	3	4	5
Общая трудоемкость	**зач. ед.**	16	4	4	4	4
	час	576	144	144	144	144
Из них:						
Часы аудиторной работы (всего):		256	64	64	64	64
Лекции		128	32	32	32	32

Практические занятия	128	32	32	32	32
Лабораторные / практические занятия по подгруппам	0	0	0	0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	320	80	80	80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)		Экзамен	Экзамен	Экзамен	Экзамен

3. Система оценивания

В течение каждого семестра студенты выполняют по 3 контрольные работы и могут набрать по 20 баллов за каждую, по окончании каждого семестра планируется проведение коллоквиума по теоретическому материалу (40 баллов).

Студенты, получившие по итогам работы в семестре не менее 61 балла, получают оценку за экзамен по дисциплине автоматически в соответствии со шкалой перевода баллов в оценки: 61-75 баллов - удовлетворительно; 76-90 баллов - хорошо; 91-100 баллов - отлично.

Студенты, не получившие оценку за экзамен по дисциплине автоматически, или желающие улучшить полученную оценку, должны сдавать экзамен.

4. Содержание дисциплины

4.1. Тематический план дисциплины

2 семестр:

Таблица 2

№	Наименование тем	Объем дисциплины, час.			
		Всего	Виды аудиторной работы (академические часы)		Иные виды контактной работы
			Лекции	Практические занятия	
1	2	3	4	5	6
1	Основные понятия. Алгебра матриц.	2	2	0	
2	Операции над матрицами.	2	0	2	
3	Определители и из свойства (лекция).	2	2	0	
4	Определители и из свойства.	4	0	2	
5	Линейные пространства.	2	2	0	
6	Контрольная работа №1.	12	0	2	
7	Ранг матриц.	2	2	0	
8	Линейные пространства.	4	0	2	
9	Системы линейных уравнений.	2	2	0	
10	Ранг матриц.	4	0	2	
11	Аксиоматика линейных пространств.	2	2	0	
12	Контрольная работа №2.	12	0	2	

13	Линейные операторы.	4	2	0	
14	Системы линейных уравнений.	4	0	2	
15	Образ и ядро линейного оператора.	2	2	0	
16	Координаты векторов.	4	0	2	
17	Евклидовы и унитарные пространства.	2	2	0	
18	Связь матриц линейного оператора в различных базисах.	4	0	2	
19	Процесс ортогонализации.	2	2	0	
20	Ранг и дефект.	4	0	2	
21	Собственные векторы и значения (лекция).	2	2	0	
22	Метод ортогонализации.	4	0	2	
23	Линейные операторы в евклидовых и унитарных пространствах.	2	2	0	
24	Собственные векторы и значения.	4	0	2	
25	Унитарные операторы.	4	2	0	
26	Контрольная работа №3.	12	0	2	
27	Эрмитовы операторы.	4	2	0	
28	Ортогональные операторы.	4	0	2	
29	Квадратичная форма (лекция).	2	2	0	
30	Квадратичные формы.	2	0	2	
31	Приведение квадратичной формы к главным осям.	4	2	0	
32	Приведение к главным осям.	2	0	2	
33	Коллоквиум.	20	0	0	
34	Консультация перед экзаменом.	2	0	0	2
35	Экзамен по курсу.	0	0	0	
	Итого во 2 семестре (часов)	144	32	32	2

3 семестр:

Таблица 3

№	Наименование тем	Объем дисциплины, час.			
		Всего	Виды аудиторной работы (академические часы)		Иные виды контактной работы
			Лекции	Практические занятия	
1	2	3	4	5	6
1	Элементы теории множеств.	2	2	0	
2	Множества.	2	0	2	
3	Последовательности.	2	2	0	
4	Предел последовательности.	4	0	2	
5	Функции.	2	2	0	
6	Предел функции.	4	0	2	
7	Непрерывные функции.	2	2	0	

8	Контрольная работа №1.	12	0	2	
9	Производная функции.	2	2	0	
10	Дифференцирование функций.	4	0	2	
11	Исследование функций.	2	2	0	
12	Построение графиков функций.	4	0	2	
13	Функции многих переменных.	4	2	0	
14	Экстремумы функций многих переменных.	4	0	2	
15	Исследование функций многих переменных.	2	2	0	
16	Интегрирование.	4	0	2	
17	Неопределенный интеграл.	2	2	0	
18	Контрольная работа №2.	12	0	2	
19	Определенный интеграл (лекция).	2	2	0	
20	Определенный интеграл.	4	0	2	
21	Дифференциальные уравнения (лекция).	2	2	0	
22	Дифференциальные уравнения.	4	0	2	
23	Дифференциальные уравнения 2 порядка (лекция).	2	2	0	
24	Дифференциальные уравнения 2 порядка.	4	0	2	
25	Числовые ряды.	4	2	0	
26	Контрольная работа №3.	12	0	2	
27	Сходимость рядов.	4	2	0	
28	Числовые ряды 1.	4	0	2	
29	Функциональные ряды.	2	2	0	
30	Числовые ряды 2.	2	0	2	
31	Степенные ряды (лекция).	4	2	0	
32	Степенные ряды.	2	0	2	
33	Коллоквиум.	20	0	0	
34	Консультация перед экзаменом.	2	0	0	2
35	Экзамен по курсу.	0	0	0	
	Итого в 3 семестре (часов)	144	32	32	2

4 семестр:

Таблица 4

№	Наименование тем	Объем дисциплины, час.			
		Всего	Виды аудиторной работы (академические часы)		Иные виды контактной работы
			Лекции	Практические занятия	
1	2	3	4	5	6
1	Основные алгебраические структуры.	2	2	0	
2	Группы. Кольца. Поля.	2	0	2	
3	Кольцо вычетов. Сравнения.	2	2	0	
4	Вычеты. Сравнения.	4	0	2	

5	Сравнение с одним неизвестным (лекция).	2	2	0	
6	Сравнения с одним неизвестным.	4	0	2	
7	Сравнения второй степени.	2	2	0	
8	Контрольная работа №1.	12	0	2	
9	Кольцо целых чисел.	2	2	0	
10	Целые числа..	4	0	2	
11	Поле комплексных чисел.	2	2	0	
12	Комплексные числа.	4	0	2	
13	Тригонометрическая форма комплексного числа (лекция).	4	2	0	
14	Тригонометрическая форма комплексного числа.	4	0	2	
15	Кольцо многочленов.	2	2	0	
16	Деление многочленов.	4	0	2	
17	Корни многочленов.	2	2	0	
18	Контрольная работа №2.	12	0	2	
19	Многочлены над произвольным полем.	2	2	0	
20	Кольцо вычетов.	4	0	2	
21	Важнейшие функции теории чисел.	2	2	0	
22	Разложение на множители.	4	0	2	
23	Трансцендентные числа.	2	2	0	
24	Функции Мёбиуса и Эйлера.	4	0	2	
25	Основные комбинаторные конфигурации.	4	2	0	
26	Элементы комбинаторики.	2	0	2	
27	Методы перечисления.	4	2	0	
28	Элементы комбинаторики.	4	0	2	
29	Производящие функции (лекция).	2	2	0	
30	Производящие функции.	2	0	2	
31	Распределение простых чисел в арифметических прогрессиях.	4	2	0	
32	Контрольная работа №3.	12	0	2	
33	Коллоквиум.	20	0	0	
34	Консультация перед экзаменом.	2	0	0	2
35	Экзамен по курсу.	0	0	0	
	Итого в 4 семестре (часов)	144	32	32	2

5 семестр:

Таблица 5

№	Наименование тем	Объем дисциплины, час.			
		Всего	Виды аудиторной работы (академические часы)		Иные виды контактной работы
			Лекции	Практические занятия	

1	2	3	4	5	6
1	Основные понятия теории графов.	2	2	0	
2	Графы.	2	0	2	
3	Остовы и деревья.	2	2	0	
4	Деревья.	4	0	2	
5	Сети. Потоки.	2	2	0	
6	Сеть. Поток. Разрез.	4	0	2	
7	Побуквенное кодирование.	2	2	0	
8	Кодирование.	4	0	2	
9	Оптимальные коды.	2	2	0	
10	Контрольная работа №1.	12	0	2	
11	Логика высказываний.	2	2	0	
12	Формулы алгебры логики.	4	0	2	
13	Булевы функции.	4	2	0	
14	Совершенные формы.	4	0	2	
15	Предполные классы булевых функций.	2	2	0	
16	Контрольная работа №2.	12	0	2	
17	Исчисление высказываний.	2	2	0	
18	Секвенции.	4	0	2	
19	Логика предикатов.	2	2	0	
20	Предикаты.	4	0	2	
21	Нормальная форма предикатов.	2	2	0	
22	Предварено нормальная форма.	4	0	2	
23	Фильтры, теорема компактности.	2	2	0	
24	Контрольная работа №3.	12	0	2	
25	Исчисление предикатов (лекция).	4	2	0	
26	Исчисление предикатов.	2	0	2	
27	Вычислимые функции (лекция).	4	2	0	
28	Вычислимые функции.	4	0	2	
29	Частично рекурсивные функции (лекция).	4	2	0	
30	Частично рекурсивные функции.	2	0	2	
31	Машина Тьюринга.	4	2	0	
32	Функции, вычислимые на машине Тьюринга.	2	0	2	
33	Коллоквиум.	20	0	0	
34	Консультация перед экзаменом.	2	0	0	2
35	Экзамен по курсу.	0	0	0	
	Итого в 5 семестре (часов)	144	32	32	2

4.2. Содержание дисциплины *(модуля)* по темам

Высшая математика 2 семестр.

1. **"Основные понятия. Алгебра матриц."**

Размещения, перестановки, сочетания. Связи между ними. Основной комбинаторный, принцип. Выборки с возвращением. Выборки без возвращения. Выборки элементов, некоторые из которых повторяются. Множество. Пустое множество. Подмножество. Собственные и несобственные подмножества множества. Равенство множеств. Внутренние бинарные операции на множестве. Объединение множеств. Пересечение. множеств. Дополнение одного множества до другого. Декартово произведение множеств. Матрица размера m x n. Квадратная матрица порядка n. Диагональная матрица. Единичная матрица порядка n. Нулевая матрица размера m x n. Вектор-строка. Вектор- столбец. Равенство матриц.

Операции над матрицами. Сложение матриц одинакового размера. Умножение матрицы на число. Транспонирование матрицы. Произведение матриц. Свойства операций над матрицами. Элементарные преобразования матриц. Определитель квадратной матрицы. Миноры и алгебраические дополнения. Теорема Лапласа. Разложение определителя по строке. Свойства определителя. Вырожденные и невырожденные матрицы. Определитель квазитреугольной матрицы. Обратная матрица. Свойства обратной матрицы.

2. **"Операции над матрицами."**

Операции над матрицами. Сложение матриц одинакового размера. Умножение матрицы на число. Транспонирование матрицы. Произведение матриц. Свойства операций над матрицами. Элементарные преобразования матриц.

3. **"Определители и их свойства." (лекция)**

Определитель квадратной матрицы. Миноры и алгебраические дополнения. Теорема Лапласа. Разложение определителя по строке. Свойства определителя. Вырожденные и невырожденные матрицы. Определитель квазитреугольной матрицы. Обратная матрица. Свойства обратной матрицы.

4. **"Определители и изх свойства." (практическое занятие)**

Определители 2-го и 3-го порядков. Свойства определителей. Теорема Лапласа. Вычисление определителй любого порядка.

5. **"Линейные пространства." (лекция)**

Линейное пространство. Примеры линейных пространств: пространство геометрических векторов, арифметическое пространство Rn. Подпространство линейного пространства. Линейная оболочка. Сумма подпространств. Пересечение подпространств. Изоморфизм линейных пространств. Линейная зависимость векторов и ее геометрический смысл. Базис линейного пространства. Размерность линейного пространства. Координаты вектора.

6. **"Контрольная работа №1."**

7. **"Ранг матриц."**

Подпространства линейных пространств. Линейная оболочка. Минорный ранг матриц. Ранг матриц по строкам и по столбцам. Эквивалентность определений ранга матриц. Теорема о ранге. Преобразования, не меняющие ранга матриц.

8. **"Линейные пространства." (практическое занятие)**

Арифметические линейные векторные пространства. Линейно зависимые и независимые системы векторов. Системы порождающих векторных пространств. Базис пространства. Координаты векторов в данном базисе.

9. **"Системы линейных уравнений." (лекция)**

Система линейных уравнений. Определение решения системы линейных уравнений. Эквивалентность систем линейных уравнений. Совместность системы линейных уравнений. Теорема Кронекера — Капелли. Однородная система линейных уравнений. Неоднородная система линейных уравнений. Система линейных уравнений с квадратной невырожденной матрицей. Правило Крамера. Исследование и решение системы линейных уравнений методом Жордана — Гаусса. Частные решения системы линейных уравнений. Элементарные преобразования системы линейных уравнений. Геометрические свойства решений системы линейных уравнений: фундаментальная система решений однородной системы линейных уравнений, линейное подпространство решений однородной системы линейных уравнений.

10. **"Ранг матриц."**

Вычисление минорного ранга матриц. Эквивалентные матрицы. Вычисление ранга по строкам и по столбцам.

11. **"Аксиоматика линейных пространств."**

Аксиоматика линейных пространств. Теорема об изоморфизме. Пересечение, сумма и прямая сумма подпространств. Теоремы о размерностях пересечения, суммы и прямой суммы подпространств. Переход к новому базису. Матрица перехода к новому базису. Преобразование координат вектора при переходе к новому базису.

12. **"Контрольная работа №2."**

13. **"Линейные операторы."**

Определение линейного оператора. Теорема о существовании и единственности линейного оператора. Связь матриц линейного оператора в различных базисах. Подобные матрицы.

14. **"Системы линейных уравнений." (практическое занятие)**

Решение систем линейных уравнений различными методами. Фундаментальная система решений системы линейных однородных уравнений.

15. **"Образ и ядро линейного оператора."**

Образ и ядро линейного оператора. Размерность образа и ядра линейного пространства, ранг и дефект линейного оператора.

16. **"Координаты векторов."**

Преобразование координат вектора при переходе к новому базису.

17. **"Евклидовы и унитарные пространства."**

Скалярное произведение. Неравенство Коши — Буняковского. Евклидово пространство. Унитарное пространство. Длина вектора в евклидовом (унитарном) пространстве. Неравенства треугольника. Ортогональные векторы. Ортогональный базис линейного пространства.

18. **"Связь матриц линейного оператора в различных базисах. "**

Подобные матрицы. Связь матриц линейного оператора в различных базисах.

19. **"Процесс ортогонализации."**

Ортонормированный базис линейного пространства. Процесс ортогонализации Грама — Шмидта. Матрица Грама. Определитель Грама. Свойства матрицы Грама и определителя Грама. Ортогональное дополнение. Линейные многообразия в евклидовом (унитарном) пространстве. Расстояние от вектора до линейного подпространства.

20. **"Ранг и дефект."**

Нахождение базиса и размерности ядра линейного оператора.

21. **"Собственные векторы и значения. "(лекция)**

Собственные значения и собственные векторы линейного оператора. Линейная независимость собственных векторов, отвечающих различным собственным значениям. Собственные значения и собственные векторы матрицы. Характеристический многочлен матрицы. Характеристический многочлен линейного оператора. Способ определения собственных векторов. Теорема о диагонализируемости.

22. **"Метод ортогонализации."**

Метод ортогонализации Грамма-Шмидта.

23. **"Линейные операторы в евклидовых и унитарных пространствах."**

Сопряженный оператор. Нормальный оператор. Теорема Шура. Критерий нормальности.

24. **"Собственные векторы и значения."**

Нахождение собственных значений и собственных векторов линейного оператора.

25. **"Унитарные операторы."**

Унитарный (ортогональный) оператор. Критерий унитарности. Спектральная характеристика унитарного оператора. Каноническая форма матрицы ортогонального оператора.

26. **"Контрольная работа №3."**

27. **"Эрмитовы операторы."**

Самосопряженные и эрмитовы операторы. Основная теорема об эрмитовых операторах.

28. **"Ортогональные операторы."**

Критерии ортогональности линейного оператора.

29. **"Квадратичная форма." (лекция)**

Квадратичная форма. Матрица квадратичной формы. Приведение квадратичной формы к каноническому виду.

30. **"Квадратичные формы."**

Приведение квадратичной формы к каноническому виду.

31. **"Приведение квадратичной формы к главным осям."**

Приведение квадратичной формы к каноническому виду ортогональным преобразованием. Распадающиеся формы. Положительно определенные формы. Пары форм.

32. **"Приведение к главным осям."**

Приведение квадратичной формы к главным осям.

33. **"Коллоквиум."**

34. **"Консультация перед экзаменом."**

35. **"Экзамен по курсу."**

Высшая математика 3 семестр.

1. **"Элементы теории множеств."**

Понятие множества и подмножества. Операции: объединение, пересечение, дополнение. Понятие действительного (вещественного) числа. Сравнение действительных чисел. Примеры множеств действительных чисел. Промежутки. Ограниченные (сверху, снизу) и неограниченные множества действительных чисел. Верхние и нижние и точные верхние и нижние грани множеств действительных чисел. Максимальный и минимальный элемент множества. Теорема о существовании точных граней у ограниченного множества. Лемма о вложенных отрезках.

2. **"Множества."**

Понятие множества и подмножества. Операции: объединение, пересечение, дополнение. Понятие действительного (вещественного) числа. Сравнение действительных чисел. Примеры множеств действительных чисел. Промежутки. Ограниченные (сверху, снизу) и неограниченные множества действительных чисел. Верхние и нижние и точные верхние и нижние грани множеств действительных чисел. Максимальный и минимальный элемент множества.

3. **"Последовательности."**

Последовательности. Примеры. Понятие предела последовательности. Теорема о единственности предела сходящейся последовательности. Ограниченные и неограниченные последовательности. Теорема об ограниченности сходящейся последовательности. Теорема о переходе к пределу в неравенствах. Теорема о сходимости монотонных ограниченных последовательностей. Определение числа e. Бесконечно малые последовательности. Связь со сходящимися последовательностями. Арифметические свойства для последовательностей, имеющих конечные и бесконечные пределы. Неопределенности. Определение подпоследовательности. Теорема о пределе подпоследовательности сходящейся последовательности. Теорема Больцано-Вейерштрасса. Критерий Коши сходимости последовательности.

4. **"Предел последовательности."**

Вычисление предела последовательности.

5. **"Функции."**

Числовые функции, характеристика общих свойств числовых функций. Обзор элементарных функций. Определение предела функции в точке в терминах окрестностей, неравенств (Коши) и последовательностей (Гейне). Теорема об эквивалентности этих определений. Односторонние пределы. Пределы функции в бесконечности. Арифметические свойства функций, имеющих пределы (конечные или бесконечные) в точке или в бесконечности. Неопределенности. Теоремы о переходе к пределу в неравенствах, о вынужденном пределе. Теорема о пределе сложной функции. Первый и второй замечательные пределы.

6. **"Предел функции."**

Вычисление пределов функций.

7. **"Непрерывные функции."**

Определение непрерывности функции в точке. Точки разрыва, их классификация. Непрерывность основных элементарных функций. Арифметические свойства непрерывных функций. Теорема о непрерывности сложной функции. Свойства функций, непрерывных на отрезке (первая и вторая теоремы Вейерштрасса, теорема Коши).

8. **"Контрольная работа №1."**

9. **"Производная функции."**

Дифференциальное исчисление функций одной переменной. Дифференцируемость функции в точке. Производная и дифференциал. Геометрический и механический смысл. Критерий дифференцируемости функций. Правила дифференцирования. Дифференцирование обратной функции и сложной функции. Инвариантность формы записи первого дифференциала. Дифференцирование элементарных функций и таблица производных. Производные и дифференциалы высших порядков. Формула Лейбница. Дифференцирование функций, заданных параметрически и неявно. Основные теоремы дифференциального исчисления (Ферма, Ролля, Лагранжа, Коши). Правило Лопиталя вычисления предела функции. Формула Тейлора. Различные формы записи остаточного члена в формуле Тейлора. Разложение основных элементарных функций по формуле Тейлора. Применение формулы Тейлора в приближенном вычислении значений функции.

10. **"Дифференцирование функций."**

Правила дифференцирования. Дифференцирование обратной функции и сложной функции. Инвариантность формы записи первого дифференциала. Дифференцирование элементарных функций и таблица производных. Производные и дифференциалы высших порядков. Формула Лейбница. Дифференцирование функций, заданных параметрически и неявно.

11. **"Исследование функций."**

Приложения дифференциального исчисления к исследованию свойств функций. Условия монотонности функции на промежутке. Локальные экстремумы функции. Достаточные условия локального экстремума в терминах первой производной, второй производной и высших производных. Глобальные экстремумы функции. Выпуклые функции. Точки перегиба. Достаточные условия выпуклости и перегиба. Асимптоты.

12. **"Построение графиков функций."**

Локальные экстремумы функции. Достаточные условия локального экстремума в терминах первой производной, второй производной и высших производных. Глобальные экстремумы функции. Выпуклые функции. Точки перегиба. Достаточные условия выпуклости и перегиба. Асимптоты.

13. **"Функции многих переменных."**

Дифференциальное исчисление функций многих переменных. Евклидово n-мерное пространство. Основные определения. Внутренние, внешние, граничные точки множества в метрическом пространстве. Дифференциальное исчисление функций нескольких переменных. Непрерывные, дифференцируемые функции в Rn. Частные производные. Дифференцирование сложной функции. Производные по направлению. Градиент. Геометрический смысл дифференциала функций двух переменных. Частные производные и дифференциалы высших порядков.

14. **"Экстремумы функций многих переменных."**

Локальный экстремум функции многих переменных. Условный экстремум функций многих переменных. Необходимое условие локального экстремума. Достаточное условие локального экстремума. Функция Лагранжа и множители Лагранжа для задачи на условный экстремум.

15. **"Исследование функций многих переменных."**

Экстремумы функций многих переменных. Локальный экстремум функции многих переменных. Условный экстремум функций многих переменных. Необходимое условие

локального экстремума. Достаточное условие локального экстремума. Функция Лагранжа и множители Лагранжа для задачи на условный экстремум.

16. **"Интегрирование."**

Замена переменных и формула интегрирования по частям. Таблица интегралов. Интегрирование рациональных функций. Интегрирование некоторых иррациональных функций, тригонометрических и других трансцендентных функций.

17. **"Неопределенный интеграл."**

Первообразная и неопределенный интеграл. Понятие первообразной функции, определенной на интервале, и неопределенного интеграла. Замена переменных и формула интегрирования по частям. Таблица интегралов. Интегрирование рациональных функций. Интегрирование некоторых иррациональных функций, тригонометрических и других трансцендентных функций.

18. **"Контрольная работа №2."**

19. **"Определенный интеграл." (лекция)**

Геометрические и физические приложения определенного интеграла. Понятие интегральной суммы для функции, заданной на отрезке, и определенного интеграла. Необходимое условие интегрируемости функции на отрезке. Суммы Дарбу, их свойства. Необходимое и достаточное условие интегрируемости функции на отрезке. Основные классы интегрируемых функций. Основные свойства определенного интеграла. Интеграл с переменным верхним пределом. Теоремы о непрерывности и дифференцируемости интеграла с переменным верхним пределом. Формула Ньютона-Лейбница. Замена переменных и формула интегрирования по частям для определенного интеграла. Приложения определенного интеграла: вычисление площади криволинейной трапеции, площади криволинейного сектора в полярных координатах, вычисление объемов.Понятие несобственных интегралов первого и второго рода. Понятия абсолютной и условной сходимости несобственного интеграла.

20. **"Определенный интеграл."**

Основные свойства определенного интеграла. Интеграл с переменным верхним пределом. Теоремы о непрерывности и дифференцируемости интеграла с переменным верхним пределом. Формула Ньютона-Лейбница. Замена переменных и формула интегрирования по частям для определенного интеграла. Приложения определенного интеграла: вычисление площади криволинейной трапеции, площади криволинейного сектора в полярных координатах, вычисление объемов.

21. **"Дифференциальные уравнения." (лекция)**

Дифференциальные дифференциальные уравнения. Понятия их порядка и решения. Задача Коши для уравнения первого порядка. Методы решения некоторых дифференциальных уравнений первого порядка (с разделяющимися переменными, однородные, линейные, Бернулли).

22. **"Дифференциальные уравнения."**

Дифференциальные уравнения первого порядка. Обыкновенные дифференциальные уравнения. Понятия их порядка и решения. Задача Коши для уравнения первого порядка. Методы решения некоторых дифференциальных уравнений первого порядка (с разделяющимися переменными, однородные, линейные, Бернулли).

23. **"Дифференциальные уравнения 2 порядка." (лекция)**

Дифференциальные уравнения второго порядка. Линейные однородные и неоднородные дифференциальные уравнения второго порядка с постоянными коэффициентами.

24. **"Дифференциальные уравнения 2 порядка."**

Линейные однородные и неоднородные дифференциальные уравнения второго порядка с постоянными коэффициентами.

25. **"Числовые ряды."**

Понятие числового ряда, сходящегося ряда и его суммы. Необходимое условие сходимости ряда.

26. **"Контрольная работа №3."**
27. **"Сходимость рядов."**

Необходимое условие сходимости ряда. Признаки сравнения для положительных рядов. Признаки Даламбера и Коши. Интегральный признак Коши. Эталонные ряды. Критерий Коши сходимости ряда. Понятие абсолютной и условной сходимости числового ряда. Признак Лейбница сходимости знакочередующихся рядов. Признаки Дирихле и Абеля. Переместительное свойство абсолютно сходящихся рядов. Умножение абсолютно сходящихся рядов. Теорема Римана для условно сходящихся рядов.

28. **"Числовые ряды 1."**

Признаки сравнения для положительных рядов. Признаки Даламбера и Коши. Интегральный признак Коши. Эталонные ряды. Критерий Коши сходимости ряда.

29. **"Функциональные ряды."**

Функциональные последовательности, их сходимость в точке и на множестве. Функциональные ряды,определение. Равномерная сходимость функциональных последовательностей, критерий Коши равномерной сходимости функциональных последовательностей. Равномерная сходимость функционального ряда, критерий Коши равномерной сходимости функционального ряда. Признак Вейерштрасса равномерной сходимости функционального ряда.

30. **"Числовые ряды 2."**

Понятие абсолютной и условной сходимости числового ряда. Признак Лейбница сходимости знакочередующихся рядов. Признаки Дирихле и Абеля. Переместительное свойство абсолютно сходящихся рядов. Умножение абсолютно сходящихся рядов. Теорема Римана для условно сходящихся рядов.

31. **"Степенные ряды." (лекция)**

Степенной ряд. Теорема Абеля, интервал и радиус сходимости степенного ряда. Вычисление радиуса сходимости степенного ряда при помощи признаков Коши и Даламбера. Непрерывность суммы степенного ряда. Теоремы о почленном интегрировании и дифференцировании степенного ряда. Разложение функций функции в степенные ряды.. Ряд Тейлора (Маклорена) функции. Необходимое и достаточное условия сходимости ряда Тейлора для заданной функции к заданной функции. Разложения в ряд Маклорена основных элементарных функций.

32. **"Степенные ряды."**

Теорема Абеля, интервал и радиус сходимости степенного ряда. Вычисление радиуса сходимости степенного ряда при помощи признаков Коши и Даламбера. Непрерывность суммы степенного ряда.

33. **"Коллоквиум."**
34. **"Консультация перед экзаменом."**
35. **"Экзамен по курсу."**

<u>Высшая математика 4 семестр.</u>

1. **"Основные алгебраические структуры."**

Полугруппы, группы, кольца, поля и их простейшие свойства.

2. **"Группы. Кольца. Поля."**

Группы. Кольца. Поля. Примеры.

3. **"Кольцо вычетов. Сравнения."**

Уравнения в кольце вычетов и сравнения. Системы линейных уравнений над кольцом вычетов.Свойства сравнений (Теорема 1 и 2). Полная и приведённая системы вычетов. Теорема Эйлера и Ферма.

4. **"Вычеты. Сравнения."**

Кольца и поля вычетов. Свойства сравнений.

5. **"Сравнение с одним неизвестным." (лекция)**

Сравнения первой степени. Система сравнений первой степени, китайская теорема об остатках. Сравнения любой степени по простому и составному модулях.

6. **"Сравнения с одним неизвестным."**

Методы решений сравнений с одним неизвестным.

7. **"Сравнения второй степени. "**

Общие свойства сравнения. Символы Лежандра и Якоби, их свойства. Случай составного модуля.

8. **"Контрольная работа №1."**

9. **"Кольцо целых чисел."**

Свойства делимости. Алгоритм Евклида и следствия из него. НОК. Связь алгоритма Евклида с непрерывными дробями. Простые числа. Каноническое разложение целых чисел.

10. **"Целые числа.."**

Делимость и деление с остатком в кольце целых чисел. Основная теорема арифметики. Уравнения в кольце вычетов и сравнения. Системы линейных уравнений над кольцом вычетов.

11. **"Поле комплексных чисел."**

Комплексное число. Алгебраическая форма комплексного числа. Комплексная плоскость. Операции над комплексными числами.

12. **"Комплексные числа."**

Вычисления в поле комплексных чисел.

13. **"Тригонометрическая форма комплексного числа." (лекция)**

Тригонометрическая форма комплексного числа. Возведение комплексного числа в натуральную степень. Формула Муавра. Извлечение корня натуральной степени из комплексного числа. Геометрическая интерпретация корней. Возведение комплексного числа в рациональную степень.

14. **"Тригонометрическая форма комплексного числа."**

Комплексная плоскость. Тригонометрическая форма комплексного числа. Возведение комплексного числа в натуральную степень. Формула Муавра. Извлечение корня натуральной степени из комплексного числа. Геометрическая интерпретация корней. Возведение комплексного числа в рациональную степень.

15. **"Кольцо многочленов."**

Многочлен над полем. Сумма многочленов. Произведение многочленов. Кольцо многочленов. Деление многочленов. Теорема о делении многочлена на многочлен с остатком. Теорема о наибольшем общем делителе многочленов. Корни многочлена. Теорема Безу. Многочлены над полем комплексных чисел. Основная теорема алгебры. Каноническое разложение многочлена над полем комплексных чисел. Теорема о равенстве многочленов. Формулы Виета. Многочлены над полем вещественных чисел. Каноническое разложение многочлена над полем вещественных чисел. Возведение матрицы в натуральную степень. Многочлен от матрицы.

16. **"Деление многочленов."**

Деление многочленов. Теорема о делении многочлена на многочлен с остатком. Теорема о наибольшем общем делителе многочленов. Корни многочлена. Теорема Безу.

17. **"Корни многочленов."**

Многочлены над полем действительных и комплексных чисел. Корни многочленов. Основная теорема алгебры. Разложение многочленов на множители. Неприводимые многочлены. Кратные корни.

18. **"Контрольная работа №2."**

19. **"Многочлены над произвольным полем."**

Многочлены над конечным полем. Интерполяционный многочлен Лагранжа. Циклотомические классы. Примитивные многочлены. Круговые многочлены. Многочлен Жегалкина.

20. **"Кольцо вычетов."**

Уравнения в кольце вычетов и сравнения. Системы линейных уравнений над кольцом вычетов.

21. **"Важнейшие функции теории чисел."**

Функция [x]. Мультипликативные функции. Вывод формул для S(n) и τ(n). Функции Мёбиуса и Эйлера, их свойства.

22. **"Разложение на множители."**

Разложение многочленов на множители.

23. **"Трансцендентные числа."**

Иррациональность числа e. Теорема Линдемана. Трансцендентность числа π Теорема Гельфонда (без доказательства) и следствие из неё.

24. **"Функции Мёбиуса и Эйлера."**

Функция [x]. Мультипликативные функции. Вывод формул для S(n) и τ(n). Функции Мёбиуса и Эйлера, их свойства.

25. **"Основные комбинаторные конфигурации."**

Выборки. Перестановки, сочетания, перестановки с повторениями, сочетания с повторениями. Биномиальные коэффициенты. Свойства биномиальных коэффициентов, биномиальная теорема. Полиномиальные коэффициенты, полиномиальная теорема. Разбиения.

26. **"Элементы комбинаторики."**

Перестановки, размещения и сочетания. Решение задач.

27. **"Методы перечисления. "**

Формулы обращения. Локально конечные частично упорядоченные множества. Метод включений и исключений. Оценки для числа элементов, не обладающих ни одним из n свойств. Формула для числа элементов, обладающих в точности m свойствами, $0 \leq m \leq n$. Формальные степенные ряды, операции над рядами.

28. **"Элементы комбинаторики."**

Перестановки, размещения и сочетания с повторениями. Решение задач.

29. **"Производящие функции." (лекция)**

Примеры применения метода производящих функций для решения комбинаторных задач. Линейные рекуррентные соотношения с постоянными коэффициентами. Теорема о решении линейных рекуррентных соотношений. Числа Фибоначчи.

30. **"Производящие функции." (практическое занятие)**

Примеры применения метода производящих функций для решения комбинаторных задач. Линейные рекуррентные соотношения с постоянными коэффициентами. Теорема о решении линейных рекуррентных соотношений. Числа Фибоначчи.

31. **"Распределение простых чисел в арифметических прогрессиях."**

Теорема Дирихле. Бесконечность простых чисел вида $4t + 3$, $4t + 1$ и $6t + 1$.

32. **"Контрольная работа №3."**

33. **"Коллоквиум."**

34. **"Консультация перед экзаменом."**

35. **"Экзамен по курсу."**

Высшая математика 5 семестр.

1. **"Основные понятия теории графов."**

Основные определения. Способы задания графов. Операции над частями графа. Графы и бинарные отношения. Достижимость. Степени вершин графа. Маршруты, пути, цепи, контуры, циклы. Расстояния в графе.

2. **"Графы."**

Способы задания графов. Операции над частями графа. Степени вершин графа. Маршруты, пути, цепи, контуры, циклы.

3. **"Остовы и деревья."**

Деревья. Свойства деревьев. Бинарные деревья поиска. Взвешенные деревья. Обход бинарных деревьев. Остовные деревья. Остовы графа. Наименьший остов.

4. **"Деревья."**

Деревья. Свойства деревьев. Бинарные деревья поиска. Взвешенные деревья. Обход бинарных деревьев.

5. **"Сети. Потоки."**

Сеть. Поток. Разрез. Алгоритм нахождения максимального потока. Сетевое планирование и поиск критического пути. Сети Петри.

6. **"Сеть. Поток. Разрез."**

Сеть. Поток. Разрез. Алгоритм нахождения максимального потока.

7. **"Побуквенное кодирование."**

Побуквенное (алфавитное) кодирование. Разделимые коды. Неравенство Крафта-Макмиллана. Условие существования разделимого р–ичного кода с заданным набором длин кодовых слов.

8. **"Кодирование."**

Побуквенное (алфавитное) кодирование. Разделимые коды. Неравенство Крафта-Макмиллана. Условие существования разделимого р–ичного кода с заданным набором длин кодовых слов.

9. **"Оптимальные коды."**

Оптимальные коды. Методы построения оптимальных кодов. Метод Шеннона.

Алгоритм Хаффмена построения оптимального двоичного кода.

10. **"Контрольная работа №1."**

11. **"Логика высказываний."**

Формулы логики высказываний. Равносильные формулы. Основные равносильности.

12. **"Формулы алгебры логики."**

Доказательство равносильностей. Равносильные преобразования формул алгебры логики.

13. **"Булевы функции."**

Функции алгебры логики. Существенные и несущественные переменные. Формулы. Представление функций формулами. Операция суперпозиции. Операция введения несущественной переменной. Замыкание множества функций. Замкнутые классы. Равенство функций. Эквивалентность формул. Элементарные функции и их свойства. Совершенная дизъюнктивная нормальная форма. Совершенная конъюнктивная нормальная форма. Полные системы функций. Достаточное условие полноты. Примеры полных систем. СКНФ. СДНФ. Полиномы Жегалкина.

14. **"Совершенные формы."**

Представление булевых функций в виде совершенных конъюнктивно, дизъюнктивно нормальных форм. Полином Жегалкина. Сокращенные формы.

15. **"Предполные классы булевых функций."**

Представление булевых функций полиномами. Линейные функции и их свойства. Функции, сохраняющие константы. Самодвойственные функции и их свойства. Монотонные функции и их свойства. Теорема Поста о полноте системы булевых функций. Возможность выделить из каждой полной системы полную подсистему, состоящую не более чем из 4-х функций. Базисы замкнутых классов. Примеры базисов в P2. Предполные классы. Свойства предполных классов в P2. Теорема Поста о конечной порожденности замкнутых классов булевых функций.

16. **"Контрольная работа №2."**

17. **"Исчисление высказываний."**

Высказывания и операции над ними. Аксиомы классического исчисления высказываний. Схемы аксиом. Правила вывода. Вывод. Выводимые формулы. Вывод из системы гипотез. Простые свойства выводимости. Примеры вывода. Вывод формулы $A \to A$. Теорема о дедукции. Тождественная истинность выводимых формул. Непротиворечивость классического исчисления высказываний. Теорема о полноте. Независимость схем аксиом исчисления высказываний. Теорема о независимости схем аксиом исчисления высказываний.

18. **"Секвенции."**

Доказательство секвенций.

19. **"Логика предикатов."**

Понятие предиката. Примеры. Логические операции над предикатами; кванторы. Теоретико-множественный смысл операций над предикатами. Условия полноты системы предикатов на конечном множестве. Формулы; свободные и связанные переменные. Модель, сигнатура модели. Значение формулы в модели. Формула, истинная в модели. Формула, истинная на множестве. Тождественно истинная формула. Правила эквивалентных преобразований формул логики предикатов.

20. **"Предикаты."**

Примеры предикатов. Эквивалентные и конгруэнтные формулы. Основные эквивалентности.

21. **"Нормальная форма предикатов."**

Приведение формул логики предикатов к предварено нормальной форме.

22. **"Предварено нормальная форма."**

Приведение формул логики предикатов к предварено нормальной форме.

23. **"Фильтры, теорема компактности."**

Фильтры, теорема компактности. Фильтры, максимальные фильтры. Теорема о вложении фильтров. Теорема об ультрафильтрах. Фильтрованные произведения, ультрапроизведения. Теорема об ультрапроизведениях. Теорема компактности. Предложение о бесконечных моделях. Нестандартные арифметики. Теорема о нестандартных арифметиках.

24. **"Контрольная работа №3."**

25. **"Исчисление предикатов."**

Аксиомы классического исчисления предикатов. Правила вывода. Выводимые формулы. Примеры вывода. Специальный вывод из системы гипотез, теорема о дедукции. Тождественная истинность выводимых формул. Непротиворечивость классического исчисления предикатов. Теорема Гёделя о полноте.

26. **"Исчисление предикатов."**

Аксиомы классического исчисления предикатов. Правила вывода. Выводимые формулы.

27. **"Вычислимые функции." (лекция)**

Вычислимые функции. Тезис Чёрча. Частично рекурсивные функции. Общерекурсивные функции. Вычислимые и перечислимые множества и их классы.

28. **"Вычислимые функции." (практическое занятие)**

Вычислимые функции. Примеры. Интерпритации.

29. **"Частично рекурсивные функции." (лекция)**

Частичные числовые функции. Простейшие функции. Операции суперпозиции и примитивной рекурсии. Примитивно рекурсивные функции. Операция минимизации. Частично рекурсивные функции, общерекурсивные функции. Тезис Чёрча. Теорема о совпадении класса частично рекурсивных функций и класса частичных числовых функций, вычислимых по Тьюрингу. Рекурсивные множества, разрешимые предикаты, рекурсивно перечислимые множества, частично разрешимые предикаты. Теорема Райса. Нормальные алгоритмы Маркова. Принцип нормализации.

30. **"Частично рекурсивные функции." (практическое занятие)**

Простейшие функции. Операции суперпозиции, примитивной рекурсии и минимизации. Доказательство примитивной рекурсивности функций.

31. **"Машина Тьюринга."**

Машина Тьюринга и универсальные функции. Машина Поста. Сводимости и степени. Сводимость по Тьюрингу, степени неразрешимости.

32. **"Функции, вычислимые на машине Тьюринга."**

Написание программ для стандартной машины Тьюринга.

33. **"Коллоквиум."**

34. **"Консультация перед экзаменом."**
35. **"Экзамен по курсу."**

Средства для проведения текущего контроля
Семестр 2.

Контрольная работа №1 (примерный вариант):

1. Вычислить определитель:

$$\left|(-1)\begin{pmatrix}1&2&3&4\\4&3&2&1\\1&2&1&2\\2&1&2&1\end{pmatrix}+\begin{pmatrix}5&5&4&6\\11&9&4&5\\9&8&3&6\\11&9&4&7\end{pmatrix}\right|$$

2. Решить систему уравнений методом Крамера:

$$\begin{cases}x_1+2x_2+3x_3=6\\x_1+4x_2+3x_3=8\\2x_1+6x_2+9x_3=17\end{cases}$$

3. Решить матричное уравнение:

$$\begin{pmatrix}2&1&2\\3&2&4\\5&3&7\end{pmatrix}\cdot X\cdot\begin{pmatrix}-1&1&-1\\-3&2&-2\\-6&3&-4\end{pmatrix}=\begin{pmatrix}1&1&1\\1&1&2\\1&2&3\end{pmatrix}$$

Контрольная работа №2 (примерный вариант):

1. Вычислить ранг матрицы:

$$\begin{pmatrix}7&-4&12&-11&2&-4\\-2&0&21&9&16&15\\3&-4&30&7&34&26\\8&-8&63&5&36&21\\15&-12&75&-6&38&17\end{pmatrix}$$

2. Решить систему линейных уравнений:

$$\begin{cases}2x_1-x_2+3x_3-7x_4=5\\6x_1-3x_2+x_3-4x_4=7\\4x_1-2x_2-2x_3+3x_4=2\\4x_1-2x_2+14x_3-31x_4=18\end{cases}$$

3. Решить систему линейных однородных уравнений:

$$\begin{cases}-2x_1+x_2+3x_3+5x_4=0\\x_1-2x_2+2x_3+x_4=0\\-3x_2+7x_3+7x_4=0\\-x_1-4x_2+12x_3+13x_4=0\end{cases}$$

Контрольная работа №3 (примерный вариант):

1.Построить матрицу линейного оператора, действующего из R_3 в R_3 по закону $A\bar{x} = [\bar{a}, \bar{x}]$, где векторы $\bar{x} = (x_1, x_2, x_3)$ и $\bar{a} = (1, 2, 3)$ заданы относительно канонического базиса.

2. Линейный оператор A действует в R_3 по закону $A\bar{x} = (x_1 - 3x_2 + 4x_3, 4x_1 - 7x_2 + 8x_3, 6x_1 - 7x_2 + 7x_3)$, где x_1, x_2, x_3 – координаты вектора $\bar{x}$ в базисе $\bar{e}_1 = (1, 0, 0)$, $\bar{e}_2 = (0, 1, 0)$, $\bar{e}_3 = (0, 0, 1)$. Найти собственные числа и собственные векторы этого оператора.

3. Доказать, что матрица $A = \begin{pmatrix} 6 & -5 & -3 \\ 3 & -2 & -2 \\ 2 & -2 & 0 \end{pmatrix}$ к диагональному виду не приводится.

Вопросы к коллоквиуму:

1. Перестановки, размещения и сочетания.
2. Множества и операции над ними. Мощность множеств.
3. Матрицы и операции над ними.
4. Определители. Теорема Лапласа.
5. Теорема о произведении определителей.
6. Теорема об обратной матрице.
7. Правило Крамера.
8. Арифметическое линейное пространство.
9. Ранг матриц. Теорема о ранге.
10. Системы линейных уравнений. Теорема Кронекера - Капелли.
11. Системы линейных однородных уравнений. Теорема о фундаментальных системах.
12. Линейные пространства, подпространства. Сумма и пересечение подпространств.
13. Евклидовы пространства.
14. Унитарные пространства.
15. Линейные операторы.
16. Ранг и дефект линейного оператора.
17. Собственные значения и векторы линейного оператора.
18. Нормальный оператор. Критерий нормальности.
19. Ортогональный оператор. Критерий ортогональности.
20. Самосопряжённый оператор.
21. Квадратичная форма и её канонический вид.
22. Приведение квадратичной формы к главным осям.

Семестр 3.

Контрольная работа №1 (примерный вариант):

1. Найти область определения функции:
2. Найти пределы последовательности:
3. Найти пределы функций:

Контрольная работа №2 (примерный вариант):

1. Найти производные функций:
2. Построить график функции:
3. Найти неопределенные интегралы

Контрольная работа №3 (примерный вариант):

1.Вычислите несобственные интегралы или установите их расходимость
2. Найти общее решение дифференциального уравнения .

Вопросы к коллоквиуму:

1. Понятие множества. Операции над множествами. Числовые множества. Понятие переменной величины и функции (отображения).
2. Действительные функции одной действительной переменной. Область определения. Сложная, обратная функция. Элементарная функция. Основные элементарные функции.
3. Бесконечно малые функции, их свойства. Теорема о связи бесконечно малой и функции, имеющей предел. Доказательство арифметических свойств пределов функций.
4. Первый замечательный предел (доказательство). Односторонние пределы. Бесконечно большие функции.
5. Предел функции на бесконечности. Предел последовательности. Второй замечательный предел.
6. Непрерывность функции. Свойства функций, непрерывных в точке. Классификация точек разрыва.
7. Эквивалентные функции. Теорема о применении эквивалентных при вычислении пределов (случай суммы, произведения, частного).
8. Производная функции в точке. Геометрический смысл. Доказательство теоремы о непрерывности функции, имеющей производную.
9. Производная функции в точке. Доказательство правил дифференцирования (случай суммы, произведения, частного).
10. Производная сложной и обратной функции (доказательства). Производная параметрически заданной функции.
11. Вывод формул таблицы производных. Производная показательно-степенной функции. Логарифмическое дифференцирование.
12. Производные высших порядков. Дифференцируемость функции. Дифференциал.
13. Приближенное вычисление значений функции. Свойства дифференциала. Инвариантность формы дифференциала. Дифференциалы высших порядков.
14. Теорема Ролля (доказательство).
15. Доказательство теоремы Лагранжа. Теорема Коши.
16. Правило Лопиталя (доказательство).
17. Вывод формулы Тейлора с остаточным членом в форме Лагранжа. Применение формулы Тейлора в вычислениях с заданной точностью.
18. Монотонность, экстремумы. Необходимое и достаточные (с доказательствами) условия экстремума.
19. Исследование поведения функции. Доказательство теоремы о выпуклости, вогнутости графика функции. Асимптоты.
20. Определение функций нескольких переменных. Понятие окрестности и области на плоскости.
21. Предел функции двух переменных. Непрерывность функции двух переменных. Свойства функций, непрерывных в замкнутой ограниченной области.
22. Частные производные. Геометрический и физический смысл.
23. Полный дифференциал функции нескольких переменных. Необходимое и достаточное условие дифференцируемости функции.

24. Производные и дифференциал сложной функции. Дифференциал сложной функции.

25. Неявные функции и их дифференцирование (теоремы существования, вывод формул).

26. Частные производные высших порядков. Дифференциалы высших порядков.

27. Экстремумы функций двух переменных. Необходимое и достаточное условия существования. Наибольшее и наименьшее значение функции в замкнутой области.

28. Условный экстремум.

Семестр 4.

Контрольная работа №1 (примерный вариант):

1. Найти НОД (6188,4709).
2. Найти каноническое разложение числа 125!
3. Вычислить τ(α) и S(α), α =2800.
4. Найти φ (5040), μ(147) и μ(143).
5. Решить сравнение 256x ≡179 (mod 337).
6. Решить систему сравнений
x ≡3(mod 8), x ≡11 (mod 20), x ≡1 (mod 15)
7. Решить сравнение 9x2 +29x +62≡O (mod 64)

Контрольная работа №2 (примерный вариант):

1. Найти тригонометрическую форму числа
2. Вычислить в поле комплексных чисел: $\sqrt[4]{-64}$
3. Найти наибольший общий делитель многочленов:

$$x^5+2x^4+2x^3-3x-2 \text{ и } x^4+2x^3+3x^2-2x-4.$$

Контрольная работа №3 (примерный вариант):

1. На книжной полке стоит 20 книг по геометрии, 12 - по теории вероятностей, 7 - по дифференциальным уравнениям и 25 по истории. Сколькими способами можно выбрать книгу по математике?
2. Сколько трехзначных чисел можно составить из цифр 2, 4, 6, если цифры в числе не повторяются?
3. В магазине имеются 6 сортов шоколадных конфет и 4 сорта карамели. Сколько различных покупок конфет одного сорта можно сделать в этом магазине?
4. Имеется 8 билетов денежно-вещевой лотереи, 6 билетов спортлото и 10 билетов автомотолотереи. Сколькими способами можно выбрать один билет спортлото или автомотолотереи?
5. Сколько можно молчить различных четырехзначных чисел, вставляя пропущенные цифры в число "*3*4"?
6. У одного студента имеется 7 книг по математике, а другого - 10. Сколькими способами они могут осуществить обмен?
7. Сколько различных трехбуквенных слов можно составить из букв слова ромб?
8. У англичан принято давать детям несколько имен. Сколькими способами можно назвать ребенка, если общее число имет равно 300, а ребенку дают не более трех разных имен?
9. Имеется 8 пар перчаток различных размеров. Сколькими способами можно выбрать из них одну перчатку на левую руку и одну на правую руку так, чтобы эти перчатки были различных размеров?
10. Лесник должен посадить 5 видов деревьев по двум лесополосам. Сколькими способами лесник может посадить деревья?

Вопросы к коллоквиуму:

1. Основные алгебраические структуры.
2. Кольцо целых чисел.
3. Кольцо вычетов.
4. Комплексные числа. Тригонометрическая форма.
5. Корни из комплексных чисел.
6. Кольцо многочленов. Алгоритм Евклида.
7. Неприводимые многочлены над полями R и C.
8. Алгоритм Евклида, НОД и НОК.
9. Непрерывные дроби. Таблицы подходящих дробей.
10. Функции [x] и {x}.
11. Мультипликативная функция. Формулы S(n) и τ(n).
12. Функция Мёбиуса.
13. Функция Эйлера.
14. Предложения 1 о сравнениях (5 свойств).
15. Предложения 2 о сравнениях (6 свойств).
16. Полная и приведённая система вычетов.
17. Теоремы Эйлера и Ферма.
18. Сравнение $ax \equiv b \pmod m$.
19. Система сравнений первой степени.
20. Сравнения $f(x) \equiv O \pmod p$.
21. Теорема Вильсона.
22. Свойства символа Лежандра.
23. Свойства символа Якоби.
24. Показатели и первообразные корни.
25. Бесконечность простых чисел вида $4t + 1$ и $6t + 1$.

Семестр 5.

Контрольная работа №1 (примерный вариант):

1. Ориентированный граф G с множеством вершин V = {1, 2, 3, 4, 5, 6, 7} задан списком дуг E.

   1) Построить реализацию графа G.

   2) Построить матрицу инцеденций графа G.

   3) Построить матрицу смежности (соседства вершин) графа G.

   {(1, 6), (2, 1), (2, 3), (3, 1), (3, 3), (3, 3), (3, 4), (3, 6), (5, 1), (5, 6), (7, 4), (7, 6)};

2. Используя алгоритм Прима, построить минимальный покрывающий остов и найти его длину.
3. Самостоятельно ориентировать граф и построить дерево кратчайших расстояний из 2 вершины.
4. Выяснить, является ли код C=(10,011,012,1212) с кодирующим алфавитом {0,1,2} однозначно декодируемым.
5. Построить по методу Хэмминга кодовое слово для сообщения $\alpha = (11101011)$.

Контрольная работа №2 (примерный вариант):

1. Составьте таблицу истинности булевой функции, реализованную данной формулой. Составьте по таблице истинности СДНФ и СКНФ:

$((x|y-)\rightarrow(z+xy-))\leftrightarrow(x-\downarrow y)$.

2. Проверьте, будут ли эквивалентны формулы, применяя следующие способы:

   a) составлением таблиц истинности;

   b) приведением формул к СДНФ или СКНФ с помощью эквивалентных преобразований.

   $x\rightarrow(y+x)$ и $(x\rightarrow y)+(x\rightarrow z)$.

3. С помощью эквивалентных преобразований приведите формулу к ДНФ, КНФ, СДНФ, СКНФ. Постройте полином Жегалкина.

$(x \vee y^{-}) \rightarrow (x^{-} + z^{-})$.

4. Найдите сокращенную, все тупиковые и минимальные ДНФ булевой функции, следующими способами:

a) методом Квайна;

b) с помощью карт Карно.

$f(0, 1, 0) = f(1, 0, 0) = f(1, 0, 1) = 0$.

Контрольная работа №3 (примерный вариант):

1. $\neg(X \rightarrow Y) \vdash X$,
2. $X, Y \vdash \neg(X \rightarrow \neg Y)$,
3. $\neg X \rightarrow Y \vdash \neg Y \rightarrow X$,.
4. $X \rightarrow Z, Y \rightarrow Z \vdash (\neg X \rightarrow Y) \rightarrow Z$,
5. $X \rightarrow Y, X \rightarrow \neg Y \vdash X \rightarrow Z$.

Вопросы к коллоквиуму:

1. Графы. Основные понятия. Способы представления графов.
2. Перечисление графов на нумерованных вершинах. Верхняя оценка для числа неизоморфных графов с q ребрами.
3. Эйлеровы циклы. Теорема Эйлера.
4. Деревья и их свойства.
5. Потоки в сетях. Максимальный поток. Минимальный разрез. Лемма о существовании максимального потока. Теорема Форда-Фалкерсона о максимальном потоке и минимальном разрезе.
6. Алгоритм нахождения максимального потока.
7. Теорема о целочисленности. Двудольные графы. Рассекающие множества. Теорема Кёнига–Эгервари о рассекающих множествах в двудольном графе.
8. Паросочетания в двудольных графах. Теорема Холла о паросочетаниях в двудольном графе.
9. Разделимые коды. Неравенство Крафта-Макмиллана. Условие существования разделимого р–ичного кода с заданным набором длин кодовых слов.
10. Свойства оптимальных р–ичных кодов. Верхняя и нижняя оценки стоимости оптимального кода.
11. Методы построения оптимальных кодов. Метод Шеннона; теорема Шеннона.
12. Свойства двоичных оптимальных кодов. Теорема редукции. Алгоритм Хаффменапостроения оптимального двоичного кода.
13. Булевы функции, КНФ и ДНФ, контактно-релейные схемы.
14. Теорема Поста о предполных классах.
15. Аксиоматика ИВ, вспомогательные леммы и теорема о полноте ИВ.
16. Формулы ЛП, их истинность в системах данной сигнатуры.
17. Предложения о конгруэнтных формулах и предваренной форме.
18. Основные эквивалентности.
19. Фильтры и ультрафильтры, две теоремы о них.
20. Теорема об ультрапроизведениях и компактности.
21. Предложения о нестандартной модели арифметики и бесконечных моделях
22. ИП. Теорема о существовании модели.
23. Теоремы о полноте ИП и независимости аксиом.
24. ЧРФ и машины Тьюринга.
25. Рекурсивно перечислимые множества. Теорема Поста. Построение простого множества.

26. Неразрешимые проблемы. Элементарная теория арифметики. Тождественно истинные формулы ИП.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 6

№ Темы	Темы	Формы СРС, включая требования к подготовке к занятиям
	2 семестр	
	Высшая математика.	
1	Основные понятия. Алгебра матриц.	Чтение обязательной и дополнительной литературы
2	Операции над матрицами.	Проработка лекций
3	Определители и из свойства. (лекция)	Чтение обязательной и дополнительной литературы
4	Определители и из свойства.	Проработка лекций
5	Линейные пространства.	Чтение обязательной и дополнительной литературы
6	Контрольная работа №1.	Проработка лекций
7	Ранг матриц.	Чтение обязательной и дополнительной литературы
8	Линейные пространства.	Проработка лекций
9	Системы линейных уравнений. (лекция)	Чтение обязательной и дополнительной литературы
10	Ранг матриц.	Проработка лекций
11	Аксиоматика линейных пространств.	Чтение обязательной и дополнительной литературы
12	Контрольная работа №2.	Проработка лекций
13	Линейные операторы.	Чтение обязательной и дополнительной литературы
14	Системы линейных уравнений.	Проработка лекций
15	Образ и ядро линейного оператора.	Чтение обязательной и дополнительной литературы
16	Координаты векторов.	Проработка лекций
17	Евклидовы и унитарные пространства.	Чтение обязательной и дополнительной литературы
18	Связь матриц линейного оператора в различных базисах.	Проработка лекций
19	Процесс ортогонализации.	Чтение обязательной и дополнительной литературы
20	Ранг и дефект.	Проработка лекций
21	Собственные векторы и значения. (лекция)	Чтение обязательной и дополнительной литературы
22	Метод ортогонализации.	Проработка лекций
23	Линейные операторы в евклидовых и унитарных пространствах.	Чтение обязательной и дополнительной литературы
24	Собственные векторы и значения.	Проработка лекций
25	Унитарные операторы.	Чтение обязательной и дополнительной литературы

26	Контрольная работа №3.	Проработка лекций
27	Эрмитовы операторы.	Чтение обязательной и дополнительной литературы
28	Ортогональные операторы.	Проработка лекций
29	Квадратичная форма.	Чтение обязательной и дополнительной литературы
30	Квадратичные формы.	Проработка лекций
31	Приведение квадратичной формы к главным осям.	Чтение обязательной и дополнительной литературы
32	Приведение к главным осям.	Проработка лекций
33	Коллоквиум.	Самостоятельное изучение заданного материала
34	Консультация перед экзаменом.	Самостоятельное изучение заданного материала
35	Экзамен по курсу.	Самостоятельное изучение заданного материала
	3 семестр	
	Высшая математика.	
1	Элементы теории множеств.	Чтение обязательной и дополнительной литературы
2	Множества.	Проработка лекций
3	Последовательности.	Чтение обязательной и дополнительной литературы
4	Предел последовательности.	Проработка лекций
5	Функции.	Чтение обязательной и дополнительной литературы
6	Предел функции.	Проработка лекций
7	Непрерывные функции.	Чтение обязательной и дополнительной литературы
8	Контрольная работа №1.	Проработка лекций
9	Производная функции.	Чтение обязательной и дополнительной литературы
10	Дифференцирование функций.	Проработка лекций
11	Исследование функций.	Чтение обязательной и дополнительной литературы
12	Построение графиков функций.	Проработка лекций
13	Функции многих переменных.	Чтение обязательной и дополнительной литературы
14	Экстремумы функций многих переменных.	Проработка лекций
15	Исследование функций многих переменных.	Чтение обязательной и дополнительной литературы
16	Интегрирование.	Проработка лекций
17	Неопределенный интеграл.	Чтение обязательной и дополнительной литературы
18	Контрольная работа №2.	Проработка лекций
19	Определенный интеграл. (лекция)	Чтение обязательной и дополнительной литературы
20	Определенный интеграл.	Проработка лекций
21	Дифференциальные уравнения. (лекция)	Чтение обязательной и дополнительной литературы

22	Дифференциальные уравнения.	Проработка лекций
23	Дифференциальные уравнения 2 порядка. (лекция)	Чтение обязательной и дополнительной литературы
24	Дифференциальные уравнения 2 порядка.	Проработка лекций
25	Числовые ряды.	Чтение обязательной и дополнительной литературы
26	Контрольная работа №3.	Проработка лекций
27	Сходимость рядов.	Чтение обязательной и дополнительной литературы
28	Числовые ряды 1.	Проработка лекций
29	Функциональные ряды.	Чтение обязательной и дополнительной литературы
30	Числовые ряды 2.	Проработка лекций
31	Степенные ряды.	Чтение обязательной и дополнительной литературы
32	Степенные ряды.	Проработка лекций
33	Коллоквиум.	Самостоятельное изучение заданного материала
34	Консультация перед экзаменом.	Самостоятельное изучение заданного материала
35	Экзамен по курсу.	Самостоятельное изучение заданного материала
	4 семестр	
	Высшая математика.	
1	Основные алгебраические структуры.	Чтение обязательной и дополнительной литературы
2	Группы. Кольца. Поля.	Проработка лекций
3	Кольцо вычетов. Сравнения.	Чтение обязательной и дополнительной литературы
4	Вычеты. Сравнения.	Проработка лекций
5	Сравнение с одним неизвестным. (лекция)	Чтение обязательной и дополнительной литературы
6	Сравнения с одним неизвестным.	Проработка лекций
7	Сравнения второй степени.	Чтение обязательной и дополнительной литературы
8	Контрольная работа №1.	Проработка лекций
9	Кольцо целых чисел.	Чтение обязательной и дополнительной литературы
10	Целые числа..	Проработка лекций
11	Поле комплексных чисел.	Чтение обязательной и дополнительной литературы
12	Комплексные числа.	Проработка лекций
13	Тригонометрическая форма комплексного числа. (лекция)	Чтение обязательной и дополнительной литературы
14	Тригонометрическая форма комплексного числа.	Проработка лекций
15	Кольцо многочленов.	Чтение обязательной и дополнительной литературы
16	Деление многочленов.	Проработка лекций

17	Корни многочленов.	Чтение обязательной и дополнительной литературы
18	Контрольная работа №2.	Проработка лекций
19	Многочлены над произвольным полем.	Чтение обязательной и дополнительной литературы
20	Кольцо вычетов.	Проработка лекций
21	Важнейшие функции теории чисел.	Чтение обязательной и дополнительной литературы
22	Разложение на множители.	Проработка лекций
23	Трансцендентные числа.	Чтение обязательной и дополнительной литературы
24	Функции Мёбиуса и Эйлера.	Проработка лекций
25	Основные комбинаторные конфигурации.	Чтение обязательной и дополнительной литературы
26	Элементы комбинаторики.	Проработка лекций
27	Методы перечисления.	Чтение обязательной и дополнительной литературы
28	Элементы комбинаторики.	Проработка лекций
29	Производящие функции. (лекция)	Чтение обязательной и дополнительной литературы
30	Производящие функции.	Проработка лекций
31	Распределение простых чисел в арифметических прогрессиях.	Чтение обязательной и дополнительной литературы
32	Контрольная работа №3.	Проработка лекций
33	Коллоквиум.	Самостоятельное изучение заданного материала
34	Консультация перед экзаменом.	Самостоятельное изучение заданного материала
35	Экзамен по курсу.	Самостоятельное изучение заданного материала
	5 семестр	
	Высшая математика.	
1	Основные понятия теории графов.	Чтение обязательной и дополнительной литературы
2	Графы.	Проработка лекций
3	Остовы и деревья.	Чтение обязательной и дополнительной литературы
4	Деревья.	Проработка лекций
5	Сети. Потоки.	Чтение обязательной и дополнительной литературы
6	Сеть. Поток. Разрез.	Проработка лекций
7	Побуквенное кодирование.	Чтение обязательной и дополнительной литературы
8	Кодирование.	Проработка лекций
9	Оптимальные коды.	Чтение обязательной и дополнительной литературы
10	Контрольная работа №1.	Проработка лекций
11	Логика высказываний.	Чтение обязательной и дополнительной литературы
12	Формулы алгебры логики.	Проработка лекций

13	Булевы функции.	Чтение обязательной и дополнительной литературы
14	Совершенные формы.	Проработка лекций
15	Предполные классы булевых функций.	Чтение обязательной и дополнительной литературы
16	Контрольная работа №2.	Проработка лекций
17	Исчисление высказываний.	Чтение обязательной и дополнительной литературы
18	Секвенции.	Проработка лекций
19	Логика предикатов.	Чтение обязательной и дополнительной литературы
20	Предикаты.	Проработка лекций
21	Нормальная форма предикатов.	Чтение обязательной и дополнительной литературы
22	Предварено нормальная форма.	Проработка лекций
23	Фильтры, теорема компактности.	Чтение обязательной и дополнительной литературы
24	Контрольная работа №3.	Проработка лекций
25	Исчисление предикатов. (лекция)	Чтение обязательной и дополнительной литературы
26	Исчисление предикатов.	Проработка лекций
27	Вычислимые функции. (лекция)	Чтение обязательной и дополнительной литературы
28	Вычислимые функции.	Проработка лекций
29	Частично рекурсивные функции. (лекция)	Чтение обязательной и дополнительной литературы
30	Частично рекурсивные функции.	Проработка лекций
31	Машина Тьюринга.	Чтение обязательной и дополнительной литературы
32	Функции, вычислимые на машине Тьюринга.	Проработка лекций
33	Коллоквиум.	Самостоятельное изучение заданного материала
34	Консультация перед экзаменом.	Самостоятельное изучение заданного материала
35	Экзамен по курсу.	Самостоятельное изучение заданного материала

6. Промежуточная аттестация по дисциплине

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

Вопросы к экзамену (2 семестр).

1. Перестановки, размещения и сочетания.
2. Множества и операции над ними. Мощность множеств.
3. Матрицы и операции над ними.
4. Определители. Теорема Лапласа.
5. Теорема о произведении определителей.
6. Теорема об обратной матрице.
7. Правило Крамера.
8. Арифметическое линейное пространство.

9. Ранг матриц. Теорема о ранге.
10. Системы линейных уравнений. Теорема Кронекера - Капелли.
11. Системы линейных однородных уравнений. Теорема о фундаментальных системах.
12. Линейные пространства, подпространства. Сумма и пересечение подпространств.
13. Евклидовы пространства.
14. Унитарные пространства.
15. Линейные операторы.
16. Ранг и дефект линейного оператора.
17. Собственные значения и векторы линейного оператора.
18. Нормальный оператор. Критерий нормальности.
19. Ортогональный оператор. Критерий ортогональности.
20. Самосопряжённый оператор.
21. Квадратичная форма и её канонический вид.
22. Приведение квадратичной формы к главным осям.

Перестановки, размещения и сочетания.

27. Множества и операции над ними. Мощность множеств.
28. Матрицы и операции над ними.
29. Определители. Теорема Лапласа.
30. Теорема о произведении определителей.
31. Теорема об обратной матрице.
32. Правило Крамера.
33. Арифметическое линейное пространство.
34. Ранг матриц. Теорема о ранге.
35. Системы линейных уравнений. Теорема Кронекера - Капелли.
36. Системы линейных однородных уравнений. Теорема о фундаментальных системах.
37. Линейные пространства, подпространства. Сумма и пересечение подпространств.
38. Евклидовы пространства.
39. Унитарные пространства.
40. Линейные операторы.
41. Ранг и дефект линейного оператора.
42. Собственные значения и векторы линейного оператора.
43. Нормальный оператор. Критерий нормальности.
44. Ортогональный оператор. Критерий ортогональности.
45. Самосопряжённый оператор.
46. Квадратичная форма и её канонический вид.
47. Приведение квадратичной формы к главным осям.

Вопросы к экзамену (3 семестр).

1. Понятие множества. Операции над множествами. Числовые множества. Понятие переменной величины и функции (отображения).
2. Действительные функции одной действительной переменной. Область определения. Сложная, обратная функция. Элементарная функция. Основные элементарные функции.
3. Бесконечно малые функции, их свойства. Теорема о связи бесконечно малой и функции, имеющей предел. Доказательство арифметических свойств пределов функций.
4. Первый замечательный предел (доказательство). Односторонние пределы. Бесконечно большие функции.
5. Предел функции на бесконечности. Предел последовательности. Второй замечательный предел.
6. Непрерывность функции. Свойства функций, непрерывных в точке. Классификация точек разрыва.
7. Эквивалентные функции. Теорема о применении эквивалентных при вычислении пределов (случай суммы, произведения, частного).

8. Производная функции в точке. Геометрический смысл. Доказательство теоремы о непрерывности функции, имеющей производную.

9. Производная функции в точке. Доказательство правил дифференцирования (случай суммы, произведения, частного).

10. Производная сложной и обратной функции (доказательства). Производная параметрически заданной функции.

11. Вывод формул таблицы производных. Производная показательно-степенной функции. Логарифмическое дифференцирование.

12. Производные высших порядков. Дифференцируемость функции. Дифференциал.

13. Приближенное вычисление значений функции. Свойства дифференциала. Инвариантность формы дифференциала. Дифференциалы высших порядков.

14. Теорема Ролля (доказательство).

15. Доказательство теоремы Лагранжа. Теорема Коши.

16. Правило Лопиталя (доказательство).

17. Вывод формулы Тейлора с остаточным членом в форме Лагранжа. Применение формулы Тейлора в вычислениях с заданной точностью.

18. Монотонность, экстремумы. Необходимое и достаточные (с доказательствами) условия экстремума.

19. Исследование поведения функции. Доказательство теоремы о выпуклости, вогнутости графика функции. Асимптоты.

20. Определение функций нескольких переменных. Понятие окрестности и области на плоскости.

21. Предел функции двух переменных. Непрерывность функции двух переменных. Свойства функций, непрерывных в замкнутой ограниченной области.

22. Частные производные. Геометрический и физический смысл.

23. Полный дифференциал функции нескольких переменных. Необходимое и достаточное условие дифференцируемости функции.

24. Производные и дифференциал сложной функции. Дифференциал сложной функции.

25. Неявные функции и их дифференцирование (теоремы существования, вывод формул).

26. Частные производные высших порядков. Дифференциалы высших порядков.

27. Экстремумы функций двух переменных. Необходимое и достаточное условия существования. Наибольшее и наименьшее значение функции в замкнутой области.

28. Условный экстремум.

Вопросы к экзамену (4 семестр).

1. Основные алгебраические структуры.
2. Кольцо целых чисел.
3. Кольцо вычетов.
4. Комплексные числа. Тригонометрическая форма.
5. Корни из комплексных чисел.
6. Кольцо многочленов. Алгоритм Евклида.
7. Неприводимые многочлены над полями R и C.
8. Алгоритм Евклида, НОД и НОК.
9. Непрерывные дроби. Таблицы подходящих дробей.
10. Функции $[x]$ и $\{x\}$.
11. Мультипликативная функция. Формулы $S(n)$ и $\tau(n)$.
12. Функция Мёбиуса.
13. Функция Эйлера.
14. Предложения 1 о сравнениях (5 свойств).
15. Предложения 2 о сравнениях (6 свойств).
16. Полная и приведённая система вычетов.

17. Теоремы Эйлера и Ферма.
18. Сравнение $ax \equiv b \pmod m$.
19. Система сравнений первой степени.
20. Сравнения $f(x) \equiv O \pmod p$.
21. Теорема Вильсона.
22. Свойства символа Лежандра.
23. Свойства символа Якоби.
24. Показатели и первообразные корни.
25. Бесконечность простых чисел вида $4t + 1$ и $6t + 1$.

Вопросы к экзамену (5 семестр).

Вопросы к экзамену.

1. Графы. Основные понятия. Способы представления графов.
2. Перечисление графов на нумерованных вершинах. Верхняя оценка для числа неизоморфных графов с q ребрами.
3. Эйлеровы циклы. Теорема Эйлера.
4. Деревья и их свойства.
5. Потоки в сетях. Максимальный поток. Минимальный разрез. Лемма о существовании максимального потока. Теорема Форда-Фалкерсона о максимальном потоке и минимальном разрезе.
6. Алгоритм нахождения максимального потока.
7. Теорема о целочисленности. Двудольные графы. Рассекающие множества. Теорема Кёнига–Эгервари о рассекающих множествах в двудольном графе.
8. Паросочетания в двудольных графах. Теорема Холла о паросочетаниях в двудольном графе.
9. Разделимые коды. Неравенство Крафта-Макмиллана. Условие существования разделимого р–ичного кода с заданным набором длин кодовых слов.
10. Свойства оптимальных р–ичных кодов. Верхняя и нижняя оценки стоимости оптимального кода.
11. Методы построения оптимальных кодов. Метод Шеннона; теорема Шеннона.
12. Свойства двоичных оптимальных кодов. Теорема редукции. Алгоритм Хаффменапостроения оптимального двоичного кода.
13. Булевы функции, КНФ и ДНФ, контактно-релейные схемы.
14. Теорема Поста о предполных классах.
15. Аксиоматика ИВ, вспомогательные леммы и теорема о полноте ИВ.
16. Формулы ЛП, их истинность в системах данной сигнатуры.
17. Предложения о конгруэнтных формулах и предваренной форме.
18. Основные эквивалентности.
19. Фильтры и ультрафильтры, две теоремы о них.
20. Теорема об ультрапроизведениях и компактности.
21. Предложения о нестандартной модели арифметики и бесконечных моделях
22. ИП. Теорема о существовании модели.
23. Теоремы о полноте ИП и независимости аксиом.
24. ЧРФ и машины Тьюринга.
25. Рекурсивно перечислимые множества. Теорема Поста. Построение простого множества.
26. Неразрешимые проблемы. Элементарная теория арифметики. Тождественно истинные формулы ИП.

6.2 Критерии оценивания компетенция:

Таблица 7

Карта критериев оценивания компетенций

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	Способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов. (ОПК-2).	Знает основные понятия, теоремы и методы алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, использующихся при изучении общетеоретических и специальных дисциплин учебного цикла; Уметет использовать знания фундаментальных основ, подходы и методы математики при решении прикладных задач; пользоваться источниками для самостоятельного изучения специальной литературы;	Контрольная работа Коллоквиум Экзамен	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимая вопроса и правильности выполнения предложенных заданий. Шкала критериев согласно требованиям п.4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература:

1. Шипачев, В. С. Высшая математика : учебник / В.С. Шипачев. — Москва : ИНФРА-М, 2021. — 479 с. — (Высшее образование). — DOI 10.12737/5394. - ISBN 978-5-16-010072-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1185673 дата обращения: 28.05.2020). – Режим доступа: по подписке.

7.2 Дополнительная литература:

1. Ржевский, С. В. Высшая математика I: линейная алгебра и аналитическая геометрия : учебное пособие / С.В. Ржевский. — Москва : ИНФРА-М, 2019. — 211 с. - ISBN 978-5-16-108269-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1065260 (дата обращения: 28.05.2020). – Режим доступа: по подписке.

2. Ржевский, С. В. Высшая математика II: дифференциальное исчисление : учебное пособие / С.В. Ржевский. — Москва : ИНФРА-М, 2019. — 257 с. - ISBN 978-5-16-108266-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1065257 (дата обращения: 28.05.2020). – Режим доступа: по подписке.

3. Ржевский, С. В. Высшая математика III: интегральное исчисление : учебное пособие / С.В. Ржевский. — Москва : ИНФРА-М, 2019. — 262 с. - ISBN 978-5-16-108267-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1065258 (дата обращения: 28.05.2020). – Режим доступа: по подписке.

4. Ржевский, С. В. Высшая математика IV: числовые и функциональные ряды; обыкновенные дифференциальные уравнения : учебное пособие / С.В. Ржевский. — Москва : ИНФРА-М, 2019. — 127 с. - ISBN 978-5-16-108268-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1065259 (дата обращения: 28.05.2020). – Режим доступа: по подписке.

7.3 Интернет-ресурсы:

1. Art of Problem Solving https://artofproblemsolving.com/.
2. Всероссийский интернет-педсовет http://pedsovet.org/.
3. Единое окно доступа к образовательным ресурсам http://window.edu.ru/.
4. Каталог статей российской образовательной прессы http://periodika.websib.ru/ .
5. Научная электронная библиотека http://elibrary.ru/.
6. Официальный сайт Министерства образования и науки Российской Федерации http://минобрнауки.рф/.
7. Российский общеобразовательный портал http://www.school.edu.ru/.
8. Сообщество взаимопомощи учителей http://pedsovet.su/.
9. Учебно-методический журнал «Математика» издательского дома «Первое сентября» http://mat.1september.ru/ .
10. Федеральный портал «Российское образование» http://www.edu.ru/ .
11. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru/.
12. Федеральный центр информационно-образовательных ресурсов http://fcior.edu.ru/.

7.4 Современные профессиональные базы данных и информационные справочные системы:

- Национальная электронная библиотека https://rusneb.ru/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю):

- Лицензионное ПО, в том числе отечественного производства:
  - платформа для электронного обучения Microsoft Teams
- Свободно распространяемое ПО, в том числе отечественного производства:
  - САПР Autodesk AutoCAD https://www.autodesk.com/free-trials;
- Лицензионное ПО:
  - платформа для электронного обучения Microsoft Teams

9. Технические средства и материально-техническое обеспечение дисциплины

Для осуществления образовательного процесса по дисциплине необходимы:

– для проведения лекционных занятий: компьютер, экран, проектор;

– для проведения практических занятий: компьютер, экран, проектор, компьютеры с выходом в интернет - из расчета 1 рабочее место не более чем на 2 студентов;

– для проведения самостоятельной работы студентов – помещения, оснащенные компьютерами с выходом в интернет.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
“01” июня 2020 г.

ДОПОЛНИТЕЛЬНЫЕ ГЛАВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Паюсова Т.И. Дополнительные главы информационной безопасности. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность» специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Дополнительные главы информационной безопасности [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Паюсова Т.И., 2020.

1. Пояснительная записка

Целью дисциплины «Дополнительные главы информационной безопасности» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой информации; систематизация знаний, а также совершенствование умений и навыков, необходимых для построения эффективной системы защиты информации.

Задачи дисциплины «Дополнительные главы информационной безопасности»: описание различных подходов к организации процесса проверки подлинности сущностей информационной безопасности; теоретическая и практическая проработка моделей разграничения прав доступа; изучение методик проведения аудита информационной безопасности и теста на проникновение; освоение методов учета и анализа действий пользователей в информационной системе; обучение навыкам решения задач информационной безопасности с помощью возможностей машинного обучения. В итоге у студентов будут сформированы следующие компетенции:

ПК-1 - способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности;

ПК-2 - способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований;

ПК-8 - способность участвовать в разработке подсистемы информационной безопасности компьютерной системы;

ПСК-3.4 - способность организовывать защиту информации в распределенных компьютерных системах.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Защита операционных систем», «Безопасность систем баз данных», «Техническая защита информации», «Модели безопасности компьютерных систем».

Дисциплина «Дополнительные главы информационной безопасности» способствует освоению следующих дисциплин: «Преддипломная практика», «Выпускная квалификационная работа (дипломная работа)».

1.2.Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-8 – способностью к самоорганизации и самообразованию		Знает: методы решения задач информационной безопасности с помощью возможностей машинного обучения. Умеет: применять методы решения задач информационной безопасности с помощью возможностей машинного обучения.
ПК-1 - способностью осуществлять подбор, изучение и обобщение		Знает: различные подходы к организации процесса проверки подлинности сущностей

научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности;		информационной безопасности; теоретическую базу моделей разграничения прав доступа; Умеет: применять различные подходы к организации процесса проверки подлинности сущностей информационной безопасности; применять модели разграничения прав доступа на практике;
ПК-2 - способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований;		Знает: методы решения задач информационной безопасности с помощью возможностей машинного обучения. Умеет: применять методы решения задач информационной безопасности с помощью возможностей машинного обучения.
ПК-8 - способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы;		Знает: методики проведения аудита информационной безопасности и теста на проникновение; методы учета и анализа действий пользователей в информационной системе; Умеет: применять методики проведения аудита информационной безопасности и теста на проникновение; применять методы учета и анализа действий пользователей в информационной системе;
ПСК-3.4 - способностью организовывать защиту информации в распределенных компьютерных системах.		Знает: различные подходы к организации процесса проверки подлинности сущностей информационной безопасности. Умеет: применять различные подходы к организации процесса проверки подлинности сущностей информационной безопасности.

* не предусмотрено

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	Всего часов (академические часы)	Часов в семестре (академические часы)
		10 семестр
Общий объем зач. ед.	5	5
час.	180	180
Из них:		
Часы аудиторной работы (всего):	64	64
Лекции	32	32
Практические занятия	32	32
Лабораторные/практические занятия по подгруппам	0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	116	116
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет

3. Система оценивания

3.1. Для текущего контроля применяется 100-балльная система оценивания. Баллы проставляются за посещение лабораторных занятий, а также активную работу на них. Результаты текущего контроля учитываются при промежуточной аттестации. Перевод баллов в зачет осуществляется по следующей шкале: от 61 до 100 баллов – «зачтено». Зачет проходит в устной форме, по билетам. В билете – 2 вопроса. Для получения оценки «зачтено» ответ студента должен показывать, что студент знает и понимает смысл и суть описываемой темы, ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Ответ может содержать небольшие недочеты.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные/практические занятия по подгруппам	
1	2	3	4	5	6	7
	Темы					
1.	Концепция AAA	8	4	4	0	0
2.	Проверка подлинности пользователей	8	4	4	0	0

3.	Протокол RADIUS	8	4	4	0	0
4.	Протокол EAP (Extensible Authentication Protocol)	8	4	4	0	0
5.	Протокол Kerberos	8	4	4	0	0
6.	Аутентификация с помощью ЭЦП	8	4	4	0	0
7.	Описание протокола IPSec	8	4	4	0	0
8.	Система PAM	4	2	2	0	0
9.	Аутентификация в ОС семейства Windows и Unix-like	4	2	2	0	0
	Итого	64	32	32	0	0

4.2. Содержание дисциплины (*модуля*) по темам

Лекция 1. Введение в информационную безопасность. Основные понятия и определения.

Определение информационной безопасности. Определение конфиденциальности, целостности и доступности информации. Определение угрозы, уязвимости и эксплойта. Словари уязвимостей. Основные способы обеспечения информационной безопасности.

Лекция 2. Классификация угроз информационной безопасности.

Классификация угроз информационной безопасности информационных систем по ряду базовых признаков: по природе возникновения, по степени преднамеренности появления, по непосредственному источнику угроз, по положению источника угроз, по степени зависимости от активности информационной системы, по степени воздействия на информационную систему и т.д.

Лекция 3. Аутентификация: проверка подлинности пользователей.

Определение аутентификации как процесса проверки подлинности субъекта. Аутентификация вида «клиент-система», сетевая аутентификация. Биометрические методы аутентификации. Аутентификация с помощью электронно-цифровой подписи. Аутентификация с помощью пары «логин/пароль». Протокол Radius, Kerberos.

Лекция 4. Авторизация: разграничение прав доступа.

Авторизация как основной механизм разграничения прав доступа. Основные модели разграничения прав доступа: дискреционная модель, мандатная модель, ролевая модель доступа, модель изолированной программной среды, модель безопасности информационных потоков.

Лекция 5. Обзор отечественных стандартов ИБ и их сравнение с зарубежными стандартами.

Объекты правового регулирования при создании и эксплуатации системы защиты информации. Использование существующих нормативных актов для создания системы информационной безопасности. Основные положения руководящих правовых документов. История создания TCSEC («Оранжевая книга»). Основные положения Руководящих документов ФСТЭК в области защиты информации. Стандарт ГОСТ Р ИСО/МЭК 15408 (на основе текста стандарта ISO 15408), обзор стандартов группы ИСО/МЭК 27000 (на основе серии стандартов ISO/IEC 27000).

Лекция 6. Структура системы защиты информации.

Комплексный подход к обеспечению информационной безопасности. Понятие политики безопасности, модели политики безопасности. Дискреционная политика безопасности. Мандатная политика безопасности. Мандатная политика целостности. Политика информационной безопасности как основа организационных мероприятий.

Контроль и моделирование как основные формы организационных действий при проверке действенности системы информационной безопасности. Разграничение прав доступа как основополагающее требование организационных мероприятий и их практическая реализация на объекте защиты.

Лекция 7. Основные элементы системы защиты информации.

Описание основных элементов системы защиты информации (IDS/IPS, SIEM, DLP, брандмауэр и т.д.).

Лекция 8. Аудит информационной безопасности.

Аудит системы информационной безопасности. Определение уровня защищённости информационной системы. Аудит системы информационной безопасности на объекте как основание для подготовки организационных и правовых мероприятий. Его критерии, формы и методы. Алгоритм проведения аудита информационной безопасности.

Лекция 9. Анализ и оценка рисков информационной безопасности.

Количественная и качественная оценки рисков. Методики анализа и оценки рисков информационной безопасности.

Планы практических занятий

Практическое занятие 1. Объекты и субъекты информационной безопасности.

Определение объектов и субъектов информационной безопасности в информационной системе.

Практическое занятие 2. Угрозы информационной безопасности.

Проведение классификации угроз информационной безопасности в информационной системе.

Практическое занятие 3. Аутентификация.

Реализация аутентификации пользователей с использованием пары «логин/пароль».

Практическое занятие 4. Авторизация.

Сравнительный анализ и реализация дискреционной, мандатной и ролевой моделей доступа.

Практическое занятие 5. Отечественные стандарты ИБ и их сравнение с зарубежными стандартами.

Обеспечение безопасности информационной системы в соответствии со стандартом ГОСТ Р ИСО/МЭК 15408 и стандартами группы ИСО/МЭК 27000.

Практическое занятие 6. Построение системы защиты информации.

Разработка и обоснование политики безопасности для информационной системы. Реализация принципа глубокой эшелонированности обороны в соответствии с комплексным подходом к обеспечению информационной безопасности.

Практическое занятие 7. Элементы системы защиты информации.

Настройка брандмауэра и IDS.

Практическое занятие 8. Аудит информационной безопасности.

Подготовка пакета документов в рамках проведения аудита информационной безопасности.

Практическое занятие 9. Анализ текущего уровня защищенности информационной системы.

Анализ защищенности системы по методу CRAMM.

Образцы средств для проведения текущего контроля

Лабораторные работы:

1. Выделить сущности (субъекты и объекты) информационной безопасности в предоставленной информационной системе.
2. Разработать модель угроз и модель злоумышленника на основании выявленных уязвимостей в информационной системе.
3. Реализовать приложение, проверяющее подлинность пользователя с помощью пары «логин/пароль».
4. Реализация дискреционной модели доступа.
5. Проектирование системы защиты информации и системы управления информационной безопасностью на базе стандарта ГОСТ Р ИСО/МЭК 15408 и стандартов группы ИСО/МЭК 27000.
6. Разработка политики безопасности.
7. Настройка правил разграничения доступа с помощью брандмауэра и настройка правил фильтрации для IDS.
8. Подготовка к аудиту информационной безопасности. Отличие аудита от теста на проникновение.
9. Анализ и оценка рисков информационной безопасности по методу CRAMM.

Темы докладов:

1. История возникновения «вирусов». Самые известные «вирусы». Структура «вируса». Принцип работы антивирусных программ;
2. Определение и структура антифрод-систем. Примеры антифрод-систем;
3. Применение систем виртуализации для обеспечения информационной безопасности;
4. SCADA-системы. Безопасность SCADA-систем;
5. Обеспечение анонимности в сети: proxy, анонимайзеры, VPN, TOR и пр.;
6. Фаззинг как средство нахождения уязвимостей и средство преодоления системы защиты;
7. Межсайтовый скриптинг (XSS): пример использования, основные цели и задачи, принцип работы XSS;
8. SQL-инъекции: основные понятия, цели и задачи «инъекции», пример;
9. Решение задач информационной безопасности с помощью возможностей машинного обучения;
10. Атака типа «отказ в обслуживании»: DoS, DDoS. Принцип построения «зомби»-сетей, основные цели атаки. Доступность как одно из ключевых свойств информации.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ Темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1	Концепция AAA (лекционное занятие)	Чтение обязательной и дополнительной литературы, изучение конспекта лекции.
2	Проверка подлинности пользователей (практическое занятие)	Выполнение лабораторной работы по теме практического занятия.

3	Протокол RADIUS (лекционное занятие)	Чтение обязательной и дополнительной литературы, изучение конспекта лекции.
4	Протокол RADIUS (практическое занятие)	Выполнение лабораторной работы по теме практического занятия.
5	Протокол EAP (Extensible Authentication Protocol) (лекционное занятие)	Чтение обязательной и дополнительной литературы, изучение конспекта лекции.
6	Протокол EAP (практическое занятие)	Выполнение лабораторной работы по теме практического занятия.
7	Протокол Kerberos (лекционное занятие)	Чтение обязательной и дополнительной литературы, изучение конспекта лекции.
8	Протокол Kerberos (практическое занятие)	Выполнение лабораторной работы по теме практического занятия.
9	Аутентификация с помощью ЭЦП (лекционное занятие)	Чтение обязательной и дополнительной литературы, изучение конспекта лекции.
10	Аутентификация с помощью ЭЦП (практическое занятие)	Выполнение лабораторной работы по теме практического занятия.
11	Описание протокола IPSec (лекционное занятие)	Чтение обязательной и дополнительной литературы, изучение конспекта лекции.
12	Протокол IPSec (практическое занятие)	Выполнение лабораторной работы по теме практического занятия.
13	Система PAM (лекционное занятие)	Чтение обязательной и дополнительной литературы, изучение конспекта лекции.
14	Система PAM (практическое занятие)	Выполнение лабораторной работы по теме практического занятия.
15	Аутентификация в ОС семейства Windows (лекционное занятие)	Чтение обязательной и дополнительной литературы, изучение конспекта лекции.
16	Аутентификация в ОС семейства Windows (практическое занятие)	Выполнение лабораторной работы по теме практического занятия.
17	Разграничение прав доступа в *nix-системах (лекционное занятие)	Чтение обязательной и дополнительной литературы, изучение конспекта лекции.
18	Разграничение прав доступа в *nix-системах (практическое занятие)	Выполнение лабораторной работы по теме практического занятия.

Порядок выполнения каждого вида самостоятельной работы:

1. Конспектирование и проработка лекционного материала.

2. Работа с основной и дополнительной литературой.
3. Анализ и проработка результатов лабораторного занятия.
4. Подготовка доклада.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения зачета – устный ответ.
Промежуточная аттестация позволяет проверить сформированность компетенций из п.1.2.
Вопросы к зачету:
1) Определение информационной безопасности (ИБ). Определение конфиденциальности, целостности и доступности. Основные подходы к обеспечению ИБ;
2) Определение «уязвимости», «угрозы», «атаки» и «эксплойта». Модели угроз и виды угроз (антропогенные, техногенные, стихийные источники угроз);
3) Модель нарушителя: определение хакерства. Цели и задачи хакера. «Белые», «серые» и «чёрные» хакеры. Социальная инженерия: определение, задачи, примеры применения для нарушения конфиденциальности, целостности и доступности информации;
4) Основные механизмы обеспечения ИБ: идентификация, аутентификация, авторизация, аудит;
5) Принципы обеспечения информационной безопасности (системности, комплексности и пр.);
6) Основная аксиома информационной безопасности. Принцип минимальных полномочий (Principle of Least Authority, POLA);
7) Закрытые, открытые и гибридные политики безопасности;
8) Парольные системы аутентификации. Стойкость парольных систем аутентификации. Взаимная проверка подлинности пользователей информационной системы;
9) Биометрические системы аутентификации. Основные методы взлома биометрических систем аутентификации;
10) Основные модели разграничения прав доступа: дискреционная, мандатная и ролевая модели доступа;
11) Принцип глубокой эшелонированности обороны. Основные элементы защиты: брандмауэры, антивирусы, IDS/IPS, DLP, SIEM;
12) Определение аудита информационной безопасности, отличие аудита от теста на проникновение;
13) Роль международных стандартов в процессе разработки национальный стандартов: международный стандарт как основа разработки национального стандарта;
14) История появления и развития стандартов информационной безопасности;
15) Обзор стандарта ISO 15408 «Общие критерии оценки безопасности информационных технологий»;
16) Обзор серии стандартов ISO/IEC 27000;

17) Определение системы управления информационной безопасностью и системы управления информационными рисками;
18) Общедоступная информация и информация ограниченного доступа согласно Федеральному закону РФ от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
19) Определения риска информационной безопасности. Формула определения величины риска. Прогнозируемые среднегодовые потери;
20) Качественная и количественная оценка рисков информационной безопасности;
21) Методики анализа и оценки рисков информационной безопасности: OCTAVE, COBRA, RiskWatch, CRAMM;
22) Управление непрерывностью бизнеса. Профиль угрозы и жизненный цикл угрозы, декларация о применимости механизмов контроля.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ПК-1 - способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности;	Знает: различные подходы к организации процесса проверки подлинности сущностей информационной безопасности; теоретическую базу моделей разграничения прав доступа; Умеет: применять различные подходы к организации процесса проверки подлинности сущностей информационной безопасности; применять модели разграничения прав доступа на практике;	Практические задания, собеседования, доклад, вопросы к зачету	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п.4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-2 - способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных	Знает: методы решения задач информационной безопасности с помощью возможностей машинного обучения. Умеет: применять методы решения задач информационной безопасности с помощью возможностей машинного обучения;	Практические задания, собеседования, доклад, вопросы к зачету	

	системах, составлять научные отчеты, обзоры по результатам выполнения исследований;			
3.	ПК-8 - способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы;	Знает: методики проведения аудита информационной безопасности и теста на проникновение; методы учета и анализа действий пользователей в информационной системе; Умеет: применять методики проведения аудита информационной безопасности и теста на проникновение; применять методы учета и анализа действий пользователей в информационной системе;	Практические задания, собеседования, доклад, вопросы к зачету	
4.	ПСК-3.4 - способностью организовывать защиту информации в распределенных компьютерных системах.	Знает: различные подходы к организации процесса проверки подлинности сущностей информационной безопасности. Умеет: применять различные подходы к организации процесса проверки подлинности сущностей информационной безопасности.	Практические задания, собеседования, доклад, вопросы к зачету	

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. **Партыка, Т. Л**. Информационная безопасность: Учебное пособие / Партыка Т. Л., Попов И. И. - 5-е изд., перераб. и доп. - Москва : Форум, НИЦ ИНФРА-М, 2016. - 432 с. (Профессиональное образование - Текст : электронный. - URL: https://znanium.com/catalog/product/516806 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

7.2. Дополнительная литература:

1. **Глинская, Е. В.** Информационная безопасность конструкций ЭВМ и систем: Учебное пособие/ГлинскаяЕ.В., ЧичваринН.В. - Москва : НИЦ ИНФРА-М, 2016. - 118 с. (Высшее образование: Бакалавриат) - Текст : электронный. - URL: https://znanium.com/catalog/product/507334 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

2. **Шаньгин, В. Ф.** Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL:

http://www.iprbookshop.ru/87995.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

7.3. Интернет-ресурсы

- Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [On-line] (дата обращения: 15.05.2020).

7.4 Современные профессиональные базы данных и информационные справочные системы:

- Национальная электронная библиотека. - https://rusneb.ru/ [On-line] (дата обращения: 15.05.2020).

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Лицензионное ПО:**
  платформа для электронного обучения Microsoft Teams;
  MS Visual Studio;
  MS SQL Server.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

- лекционная аудитория с проектором;
- компьютерный класс.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
“01” июня 2020 г.

ЗАЩИТА ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И ПЕРСОНАЛЬНЫХ ДАННЫХ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Зулькарнеев И.Р. Защита государственных информационных систем и персональных данных. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины «защита государственных информационных систем и персональных данных» опубликована на сайте ТюмГУ: Программно-аппаратные средства обеспечения информационной безопасности [электронный ресурс] / Режим доступа: https://www.utmn.ru/sveden/education/#

© Тюменский государственный университет, 2020.
© Зулькарнеев И.Р., 2020.

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОК-8, ПК-6,7,16, ПСК-3.5.*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Защита государственных информационных систем и персональных данных

В результате освоения дисциплины "Защита государственных информационных систем и персональных данных" обучающийся должен

Знать:

- основные понятия в области защиты защиты государственных информационных систем и персональных данных
- необходимость, принципы и методы защиты государственных информационных систем и персональных данных
- основные положения НПА в области защиты государственных информационных систем и персональных данных
- правила определения нарушителей и угроз безопасности информации
- правила формирования перечня мер по защите информации
- правила выбора компенсирующих мер
- правила выбора необходимых средств защиты информации

Уметь:

- определять уровень защищенности информационных систем персональных данных
- моделировать угрозы и нарушителей безопасности информации в соответствии с требованиями ФСТЭК России и ФСБ России
- формировать перечни требований и мер по защите информации
- разрабатывать техническое задание и проект на внедрение системы защиты информации
- осуществлять подбор средств защиты информации в зависимости от требований

Владеть:

- навыками сбора и подготовки исходных данных об информационной системе
- навыками использования специального ПО для создания схем в области ИБ
- навыками определения организационной и технической реализации мер по защите информации
- навыками анализа выбора компенсирующих мер по защите информации
- навыками написания официальных писем и запросов юридическим лицами

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			10
	зач. ед.	4	4

Общая трудоемкость	**час**	144	144
Из них:			
Часы аудиторной работы (всего):		64	64
Лекции		32	32
Практические занятия		32	32
Лабораторные / практические занятия по подгруппам		0	0
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Экзамен

3. Содержание дисциплины

Таблица 2

№	Тематика учебных встреч	Виды аудиторной работы (в ак.час.)			Итого аудиторных ак.часов по теме
		Лекции	Практические занятия	Лабораторные / практические занятия по подгруппам	
1	2	3	4	5	6
	Часов в 9 семестре	32	32	0	64
	Защита государственных информационных систем и персональных данных	32	32	0	64
1	Необходимость защиты ПДн и ГИС	2	0	0	2
2	Законодательство по защите ПДн	2	0	0	2
3	Основные понятия защиты ПДн	2	0	0	2
4	Основание обработки ПДн в организации	0	2	0	2
5	Права и условия обработки ПДн	2	0	0	2
6	Регуляторы в сфере ПДн	2	0	0	2
7	Информационные системы персональных данных	2	0	0	2
8	Определение уровня защищенности ИСПДн	0	2	0	2
9	Государственные информационные системы. Классификация	2	0	0	2
10	Обследование информационных систем	2	0	0	2
11	Описание ИС	0	2	0	2
12	Описание технологического процесса	0	2	0	2
13	Коллоквиум 1	0	0	0	0
14	Модель нарушителя безопасности информации	2	0	0	2
15	Построение модели нарушителя безопасности информации	0	2	0	2
16	Построение модели нарушителя безопасности информации	0	2	0	2
17	Модель угроз безопасности информации	2	0	0	2
18	Построение модели угроз	0	2	0	2
19	Построение модели угроз	0	2	0	2
20	Требования по защите информации	2	0	0	2
21	Требования по защите информации	2	0	0	2

22	Требования по защите информации	2	0	0	2
23	Формирование перечня требований и мер по защите ИС	0	2	0	2
24	Формирование перечня требований и мер по защите ИС	0	2	0	2
25	Выбор компенсирующих мер	0	2	0	2
26	Проектирование системы защиты ГИС и ИСПДн	2	0	0	2
27	Разработка проекта системы защиты ГИС	0	2	0	2
28	Выбор средств защиты информации	2	0	0	2
29	Разработка проекта системы защиты ГИС	0	2	0	2
30	Аттестация ГИС и ИСПДн	2	0	0	2
31	Коллоквиум 2	0	0	0	0
32	Защита проектов СЗИ студентов	0	2	0	2
33	Защита проектов СЗИ студентов	0	2	0	2
34	Защита проектов СЗИ студентов	0	2	0	2
35	Консультация	0	0	0	0
	Итого (ак.часов)	32	32	0	64

4. Система оценивания.

Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (135-балльной) и традиционной (4-балльной) систем оценок.

Экзаменационная оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических занятий, индивидуальных домашних заданий, контрольной работы, коллоквиумов и тестов. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

130 - 135 баллов – отлично;

115 - 129 баллов - хорошо;

Студент, у которого сумма набранных баллов, оказалась меньше 115, должен сдать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 теоретических вопроса и 1 практический. Для получения оценки «удовлетворительно» студентом должно быть сдано минимум 80% практических работ и сделан ответ на 2 вопроса из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы, и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен сдать минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен детально раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы, и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен сдать все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Скрипник, Д. А. Обеспечение безопасности персональных данных: учебное пособие / Д. А. Скрипник. — 2-е изд. — Москва : ИНТУИТ, 2016. — 121 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100272 (дата обращения: 10.05.2020). - Режим доступа: для авторизир. пользователей.
2. Персональные данные в государственных информационных ресурсах / М.Ю. Брауде-Золотарёв [и др.].. — Москва : Дело, 2016. — 55 c. — ISBN 978-5-7749-1121-9. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/51053.html (дата обращения: 24.04.2022). — Режим доступа: для авторизир. пользователей

5.2 Электронные образовательные ресурсы:

1. https://bdu.fstec.ru/

6. Современные профессиональные базы данных и информационные справочные системы:

- Institute of Electrical and Electronics Engineers, Inc (IEEE) https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) https://icdlib.nspu.ru/
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА https://rusneb.ru/
- Справочная правовая система КонсультантПлюс http://www.consultant.ru/

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

MS Office, платформа для электронного обучения Microsoft Teams.

8. Технические средства и материально-техническое обеспечение дисциплины

Мультимедийная учебная аудитория для проведения занятий лекционного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

Учебная аудитория для проведения занятий лекционного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
“01” июня 2020 г.

ЗАЩИТА КОРПОРАТИВНЫХ СИСТЕМ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность (специалитет)»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Оленников А.А. Защита корпоративных систем. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность (специалитет)», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.
Рабочая программа дисциплины опубликована на сайте ТюмГУ: Защита корпоративных систем [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Оленников А.А., 2020.

1. Пояснительная записка

Защита программ и данных обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Цель дисциплины «Защита корпоративных систем» является изучение программных способов и методов защиты современных сетевых сервисов и протоколов маршрутизации, а также - изучение основных подходов к эксплуатации технологий защиты при передаче информации в сети предприятия.

Задачи курса:

• Анализ принципов функционирования и защиты современных протоколов маршрутизации в сети предприятия;

• Организация безопасных базовых сервисов в сети предприятия средствами современного телекоммуникационного оборудования;

• Изучение функциональных возможностей современных технологий защиты передачи информации в сети предприятия.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Языки программирования», «Защита корпоративных систем».

Дисциплина «Защита программ и данных» способствует освоению преддипломной практики, защиты выпускной квалификационной работы (дипломная работа).

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ПСК-3.2 - способность анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем		знает Угрозы нарушения информационной безопасности компьютерных сетей Основные криптографические методы защиты информации Архитектуру и функции систем управления сетями, стандарты систем управления умеет Применять основные протоколы и технологии обеспечения безопасности компьютерных сетей Выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств Осуществлять диагностику и поиск неисправностей всех компонентов сети Выполнять действия по устранению неисправностей
ПСК-3.3 - способность использовать современные среды и технологии, разработки программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности		знает Угрозы нарушения информационной безопасности компьютерных сетей Основные криптографические методы защиты информации Архитектуру и функции систем управления сетями, стандарты систем управления Принципы функционирования защищенных

		сетевых протоколов Средства мониторинга и анализа компьютерных сетей Методы устранения неисправностей в технических системах умеет Применять основные протоколы и технологии обеспечения безопасности компьютерных сетей Выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств Осуществлять диагностику и поиск неисправностей всех компонентов сети Выполнять действия по устранению неисправностей
ПСК-3.5 - способность участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем		знает Угрозы нарушения информационной безопасности компьютерных сетей Основные криптографические методы защиты информации Архитектуру и функции систем управления сетями, стандарты систем управления Принципы функционирования защищенных сетевых протоколов Средства мониторинга и анализа компьютерных сетей Методы устранения неисправностей в технических системах умеет Применять основные протоколы и технологии обеспечения безопасности компьютерных сетей Выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств Осуществлять диагностику и поиск неисправностей всех компонентов сети Выполнять действия по устранению неисправностей

* не предусмотрено

2. **Структура и объем дисциплины**

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		9 семестр
Общий объем зач. ед.	4	4
час.	144	144
Из них:		
Часы аудиторной работы (всего):	64	64
Лекции	32	32
Лабораторные занятия	32	32
Практические занятия по подгруппам		
Часы внеаудиторной работы,	80	80

включая самостоятельную работу обучающегося		
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		Экзамен

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№	Наименование тем и/или разделов	Объем дисциплины (модуля), час				
		Всего	Виды аудиторной работы (в час)			Иные виды контактной работы
			Лекции	Практические занятия по подгруппам	Лабораторные занятия	
1	2	3	4	5	6	7
1.	Защита программ и данных в компьютерной сети.	17	4	0	4	0
2.	Маршрутизация в сети предприятия.	17	4	0	4	0
3.	Статические маршруты для IPv4 / IPv6	17	4	0	4	0
4.	Защита протокола RIP.	17	4	0	4	0
5.	Защита протокола EIGRP.	17	4	0	4	0
6.	Защита протокола OSPF.	17	4	0	4	0
7.	Подключение сети предприятия к сети Интернет с использованием протокола BGP.	17	4	0	4	0
8.	Защита основных сервисов сети предприятия	13	2	0	2	0
9.	Защита передаваемых по сети данных.	12	2	0	2	0
	Итого (часов)	144	32	0	32	0

4.2. Содержание дисциплины (*модуля*) по темам

1. Защита программ и данных в компьютерной сети.
Дизайн сети предприятия. Особенности сетевых приложений. Канальные среды.
2. Маршрутизация в Cisco IOS. CEF. Механизмы манипуляции маршрутной информацией. Policy Base Routing.
3. Статические маршруты для IPv4 / IPv6.
Особенности использования. Виды статических маршрутов. Варианты применения.
4. Защита протокола RIP.
Базовый функционал безопасной работы протоколов динамической маршрутизации. Особенности работы протокола RIPv2.
5. Защита протокола EIGRP.

EIGRP RTP. Манипуляции с маршрутами в EIGRP. Расширенный функционал аутентификации в EIGRP Named Mode.

6. Защита протокола OSPF.

Типы LSA в OSPFv2. OSPFv2 LSDB. Манипуляции с маршрутами в OSPFv2.
Шифрование маршрутной информации IPSEC в протоколе OSPFv3.

7. Подключение сети предприятия к сети Интернет с использованием протокола BGP.

Безопасность сети предприятия в стыках с сетью Интернет. Атрибуты BGP. BGP AF-Mode.

8. Защита основных сервисов сети предприятия.

Протоколы динамической конфигурации хоста DHCPv4 / DHCPv6. Служба доменных имен DNS. Протокол удаленного управления SSH.

9. Защита передаваемых по сети данных.

Простой протокол передачи файлов TFTP. Аутентификация и авторизация в протоколе FTP. Шифрование трафика протоколом SCP.

Планы практических занятий

Практическая работа № 1-2. Настройка канальных среды в Cisco IOS / Huawei VRP.
Конфигурирование протоколов HDLC, PPP, Frame Relay. Особенности построения туннелей GRE и DMVPN.

Практическая работа № 3-4. Policy Base Routing в Cisco IOS / Huawei VRP.
Конфигурирование access-list, prefix-list, distribute-list, route-map.

Практическая работа № 5-6. Static Routing в Cisco IOS / Huawei VRP.
Конфигурирование маршрутов по умолчанию, суммарных и плавающих статических маршрутов.

Практическая работа № 7-8. RIP в Cisco IOS / Huawei VRP.
Конфигурирование ключевых цепочек и аутентификации. Определение пассивных интерфейсов и включение запрета на получения update-сообщений.

Практическая работа № 9-10. EIGRP в Cisco IOS.
Конфигурация безопасной работы протокола EIGRP в классическом (Classic Mode) и именованном режимах (Named Mode).

Практическая работа № 11-12. OSPFv2 / OSPFv3 в Cisco IOS / Huawei VRP.
Конфигурация безопасной работы протокола OSPF в режимах: OSPFv2 / OSPFv3 Classic Mode и OSPFv3 AF-mode.

Практическая работа № 13-14. BGP в Cisco IOS. Работа с атрибутами BGP в Cisco IOS / Huawei VRP.
Конфигурирование BGP. Работа с атрибутами BGP. Настройка BGP AF-Mode.

Практическая работа № 15. DHCPv4 / DHCPv6, DNS, SSH в Cisco IOS / Huawei VRP.
Конфигурирование и защита DHCPv4. Настройка автоконфигурации хостов с технологией SLAAC и DHCPv6 с отслеживанием состояния и без отслеживания состояния. Конфигурирование DNS-сервера на маршрутизаторах. Тонкие настройки безопасного подключения по SSH.

Практическая работа № 16. TFTP. FTP. SCP в Cisco IOS / Huawei VRP.
Конфигурирование TFTP, FTP, SCP-серверов на коммуникационном оборудовании. Безопасное резервирование настроек и обновление операционных систем коммуникационных устройств.

Образцы средств для проведения текущего контроля

Проверка качества подготовки в течение семестра предполагает следующие виды промежуточного контроля:
А) модели сети на Packet Tracer;

Б) выполнение расчетной работы на компьютере в группах;

Примерные темы расчетных работ - моделей сети для Packet Tracer:

- Защита программ и данных в компьютерной сети.
- Маршрутизация в сети предприятия.
- Статические маршруты для IPv4 / IPv6
- Защита протокола RIP.
- Защита протокола EIGRP.
- Защита протокола OSPF.
- Подключение сети предприятия к сети Интернет с использованием протокола BGP.
- Защита основных сервисов сети предприятия
- Защита передаваемых по сети данных.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Защита программ и данных в компьютерной сети.	Чтение обязательной литературы, подготовка к практическим занятиям
2.	Маршрутизация в сети предприятия.	Чтение обязательной литературы, подготовка к практическим занятиям
3.	Статические маршруты для IPv4 / IPv6	Чтение обязательной литературы, подготовка к практическим занятиям
4.	Защита протокола RIP.	Чтение обязательной литературы, подготовка к практическим занятиям
5.	Защита протокола EIGRP.	Чтение обязательной литературы, подготовка к практическим занятиям
6.	Защита протокола OSPF.	Чтение обязательной литературы, подготовка к практическим занятиям
7.	Подключение сети предприятия к сети Интернет с использованием протокола BGP.	Чтение обязательной литературы, подготовка к практическим занятиям
8.	Защита основных сервисов сети предприятия	Чтение обязательной литературы, подготовка к практическим занятиям
9.	Защита передаваемых по сети данных.	Чтение обязательной литературы, подготовка к практическим занятиям

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение рекомендованной основной и дополнительной литературы.
3. Разбор примеров практических работ.

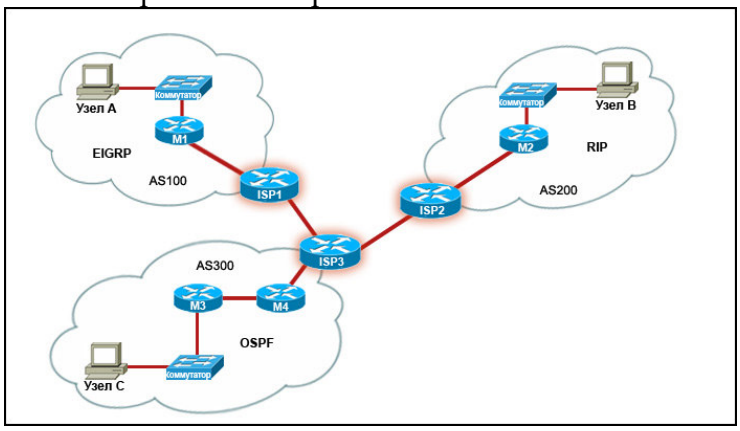
Контроль за самостоятельной работой осуществляется при выполнении обучающимся теста, контрольной работы.

6. Промежуточная аттестация по дисциплине (модулю)

Форма проведения зачета – контрольная работа.

Пример заданий на контрольную работу

1. Посмотрите на изображение.



Какой метод чаще всего используется крупными поставщиками услуг Интернета, такими как ISP1, ISP2 и ISP3, для обработки данных маршрутизации и обмена ими?

- статические маршруты
- протоколы IGP
- протоколы EGP+
- маршруты с прямым подключением

2. Какая характеристика является характеристикой протокола маршрутизации EIGRP?

- Он имеет ограничение на число переходов, которое делает протокол пригодным только для сетей, включающих менее 15 переходов.
- Обновления маршрутизации этого протокола не включают маску подсети.
- Он строит таблицу топологии на основе всех объявлений от соседних устройств.+
- Он ведет полную базу данных удаленных маршрутизаторов и методов их соединения.

3. При поиске и устранении неполадок подключения к WAN между главным офисом и офисами филиалов клиента специалист поставщика услуг Интернета проверяет конфигурацию маршрутизатора, чтобы убедиться, что она не была изменена (относительно исходной) сетевым администратором клиента. Какой тип оборудования представляет маршрутизатор?

- CPE+
- POP
- IXP
- устройство CSU/DSU

4. Посмотрите на изображение.

```
RTA# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    10.0.0.0/8 [120/2] via 192.168.1.226, 00:00:17, Serial0/0/0
     192.168.1.0/26 is subnetted, 2 subnets
C       192.168.1.64 is directly connected, FastEthernet0/0
C       192.168.1.192 is directly connected, Serial0/0/0
R    192.168.2.0/24 [120/1] via 192.168.1.226, 00:00:17, Serial0/0/0
R    192.168.3.0/24 [120/1] via 192.168.1.226, 00:00:17, Serial0/0/0
RTA#
```

Укажите часть таблицы маршрутизации, в которой задается вектор в алгоритме маршрутизации на базе вектора расстояния.

- административное расстояние
- шлюз "последней надежды"
- IP-адрес следующего перехода+
- количество переходов

Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ПСК_3.3 - способностью использовать современные среды и технологии, разработки программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности	знает Угрозы нарушения информационной безопасности компьютерных сетей Основные криптографические методы защиты информации Архитектуру и функции систем управления сетями, стандарты систем управления Принципы функционирования защищенных сетевых протоколов Средства мониторинга и анализа компьютерных сетей Методы устранения неисправностей в технических системах умеет Применять основные протоколы и технологии обеспечения безопасности компьютерных сетей Выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств Осуществлять диагностику и поиск неисправностей всех	- Опрос на практическом занятии - Тест закрытый, 10 заданий, - Тест открытый, 10 заданий, - Задачи	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

		компонентов сети Выполнять действия по устранению неисправностей		

* - не предусмотрен

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 368 c. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100522 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

7.2. Дополнительная литература:

1. Кияев, В. И. Безопасность информационных систем : учебное пособие / В. И. Кияев, О. Н. Граничин. — 2-е изд. — Москва : ИНТУИТ, 2016. — 191 c. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100580 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.
2. Олифер, В. Г. Основы сетей передачи данных : учебное пособие / В. Г. Олифер, Н. А. Олифер. — 2-е изд. — Москва : ИНТУИТ, 2016. — 219 c. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100346 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.
3. Построение коммутируемых компьютерных сетей : учебное пособие / Е. В. Смирнова, И. В. Баскаков, А. В. Пролетарский, Р. А. Федотов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 428 c. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100370 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

7.3. Интернет-ресурсы

1. Интернет ресурсы Academy Cisco http://netacad.com

7.4 Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) https://icdlib.nspu.ru/
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА https://rusneb.ru/
- Справочная правовая система КонсультантПлюс http://www.consultant.ru/

Наименование ПО

- Microsoft Office 365
- "Microsoft Imagine Academy (ранее Dreamspark):MS Visual Studio, MS SQL Server,ОС семейства MS Windows,MS Visio, MS Project"

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

эмулятор сетей PacketTracer.версия 7.x;

эмулятор сетей GNS3 2.*
эмулятор сетей eNSP 1.3.*
гипервизор Oracle Virtual Box 5.*
платформа для электронного обучения Microsoft Teams

Интернет, доступ в информационно-образовательную среду ТюмГУ, включающую в себя доступ к учебным планам и рабочим программам, к изданиям электронной библиотечной системы.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Компьютерный класс с выходом в интернет и стандартное лабораторное и периферийное оборудование классом не ниже чем в приведенной ниже конфигурации.

- 3 маршрутизатора Cisco 2801 с Base IP IOS, 128 Мбайт DRAM, 32 Мбайта флэш-памяти и модулями HWIC-2A/S;
- 3 коммутатора Cisco Catalyst 2960;
- Набор последовательных кабелей и витой пары;
- 2 беспроводных маршрутизатора Linksys (предпочтительно Linksys WRT150N; допустимо использование моделей WRT54G, WRT300N и WRT350N) или аналогичные устройства SOHO;

Для проведения лекционных и практических занятий необходим проектор с разрешением не менее 800x1200 подключенный к компьютеру с выходом в Интернет.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
“01” июня 2020 г.

Наименование дисциплины Научно-проектный (исследовательский) семинар
Рабочая программа
10.05.01 «Компьютерная безопасность (специалитет)»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Оленников А.А. Научно-проектный (исследовательский) семинар. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность (специалитет)» специализация «Безопасность распределенных компьютерных систем», специализация «Обеспечение информационной безопасности распределенных информационных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Научно-проектный (исследовательский) семинар [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Оленников А.А., 2020.

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ОК-8, ОПК-4, ПК-1.

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Научно-проектный (исследовательский) семинар

В результате изучения дисциплины студент будет
знать:

- правила оформления отчета по курсовой работе;
- правила оформления списка литературы;
- основные научные проблемы в области ИБ;

уметь:

- применять методы научных исследований в профессиональной деятельности;
- осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности;

владеть:

- навыками проведения научно-исследовательской работы;
- навыками разработки научно-технических отчетов, обзоров, публикаций по результатам выполненных работ.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**	
			7	8
Общая трудоемкость	**зач. ед.**	9	4	5
	час	324	144	180
Из них:				
Часы аудиторной работы (всего):		52	26	26
Лекции		16	8	8
Практические занятия		36	18	18
Лабораторные / практические занятия по подгруппам		0	0	0
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		272	118	154
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Зачет	Зачет

3. Содержание дисциплины

Таблица 2

№	Тематика учебных встреч	Виды аудиторной работы (в ак.час.)			Итого аудиторных ак.часов по теме
		Лекции	Практические занятия	Лабораторные / практические занятия по подгруппам	
1	2	3	4	5	6
	Часов в 7 семестре	8	10	0	18
	Научно-проектный (исследовательский) семинар	8	10	0	18
1	Актуальные проблемы и научно-исследовательские задачи в области ИБ	2	0	0	2
2	Презентация и обсуждение тем проектов	0	2	0	2
3	Поиск и систематизация научной информации. Работа с литературой.	2	0	0	2
4	Представление и обсуждение литературного обзора по теме проекта	0	2	0	2
5	Консультация	0	0	0	0
6	Подготовка научно-технического отчета	2	0	0	2
7	Презентация и обсуждение плана реализации проекта	0	2	0	2
8	Правила презентации научного исследования	2	0	0	2
9	Презентация и обсуждение промежуточных результатов реализации проекта	0	2	0	2
10	Презентация и обсуждение результатов реализации проекта	0	2	0	2
11	Консультация	0	0	0	0
12	Защита проекта	0	0	0	0
	Итого (ак.часов) в 7 семестре	8	10	0	18
	Часов в 8 семестре	8	10	0	18
	Научно-проектный (исследовательский) семинар	8	10	0	18
1	Актуальные проблемы и научно-исследовательские задачи в области ИБ	2	0	0	2

2	Презентация и обсуждение тем проектов	0	2	0	2
3	Поиск и систематизация научной информации. Работа с литературой.	2	0	0	2
4	Представление и обсуждение литературного обзора по теме проекта	0	2	0	2
5	Консультация	0	0	0	0
6	Подготовка научно-технического отчета	2	0	0	2
7	Презентация и обсуждение плана реализации проекта	0	2	0	2
8	Правила презентации научного исследования	2	0	0	2
9	Презентация и обсуждение промежуточных результатов реализации проекта	0	2	0	2
10	Презентация и обсуждение результатов реализации проекта	0	2	0	2
11	Консультация	0	0	0	0
12	Защита проекта	0	0	0	0
	Итого (ак.часов) в 8 семестре	8	10	0	18
	Итого (ак.часов)	16	20		36

4. Система оценивания.

Обучающиеся, не набравшие 61 балла в течение семестра, или не согласные с оценкой, полученной по итогам текущего контроля в семестре, проходят промежуточную аттестацию в форме дифференцированного зачета.

При проведении промежуточной аттестации результаты, полученные обучающимся в семестре, переводятся в формат традиционной оценки в соответствии со шкалой перевода баллов:

– 60 баллов и менее – «неудовлетворительно»;
– от 61 до 75 баллов – «удовлетворительно»;
– от 76 до 90 баллов – «хорошо»;
– от 91 до 100 баллов – «отлично».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Шаньгин В.Ф. Информационная безопасность и защита информации / Шаньгин В.Ф.. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87995.html (дата обращения: 24.04.2022). — Режим доступа: для авторизир. пользователей

5.2 Электронные образовательные ресурсы:

- *Institute of Electrical and Electronics Engineers, Inc (IEEE)* *https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true*
- *МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ)* *https://icdlib.nspu.ru/*
- *НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА* *https://rusneb.ru/*

6. Современные профессиональные базы данных и информационные справочные системы:

- Справочная правовая система КонсультантПлюс http://www.consultant.ru/

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

MS Office, платформа для электронного обучения Microsoft Teams.

8. Технические средства и материально-техническое обеспечение дисциплины

Мультимедийная учебная аудитория для проведения занятий лекционного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

Мультимедийная учебная аудитория для проведения занятий семинарского типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
“01” июня 2020 г.

ОРГАНИЗАЦИЯ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ МАШИН И ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Бабич А.В Организация электронно-вычислительных машин и вычислительных систем. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа составлена в соответствии с требованиями ФГОС ВО, утвержденным Приказом Министерства образования и науки РФ от 01.12.2016 г. №1512 «Об утверждении федерального государственного стандарта высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалитета)».

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Организация электронно-вычислительных машин и вычислительных систем [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Бабич А.В, 2020.

1. Пояснительная записка

Учебная дисциплина «Организация электронно-вычислительных машин и вычислительных систем» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Цель дисциплины «Организация электронно-вычислительных машин и вычислительных систем» обучить студентов общим принципам построения и эксплуатации аппаратных средств вычислительной техники и методов ее функционирования в локальных и глобальных вычислительных сетях.

Задачи дисциплины:

- обучение студентов систематизированным представлениям о принципах построения и архитектурных особенностях различных классов электронно-вычислительных машин (ЭВМ);
- изложение основных концепций, представления, хранения и обработки данных в ЭВМ;
- изучение принципов работы микропроцессорных систем.

1.1. Место дисциплины в структуре образовательной программы

Данная дисциплина входит в блок Б1, Базовая часть. Дисциплина является вводной и основополагающей для дисциплин компьютерного цикла, определенных стандартом министерства высшего и профессионального образования России по специальности «Компьютерная безопасность».

Дисциплина является базовой для изучения курсов по операционным системам и вычислительным сетям. Знания, умения и практические навыки, полученные в результате изучения дисциплины «Организация электронно-вычислительных машин и вычислительных систем», используются студентами при изучении естественно-научных дисциплин, а также при разработке курсовых и дипломных работ.

1.2.Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОПК-7 - способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения		**Знает**: основные этапы создания и развития ЭВМ; существующие виды архитектур ЭВМ, назначение и функции ее элементов; структуру и принципы работы современных и перспективных микропроцессоров; основы языка низкого уровня (язык ассемблера). **Умеет**: работать с современной элементной базой электронной аппаратуры; определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав параметры периферийных устройств.

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы		Всего часов (академические часы)	Часов в семестре (академические часы)	
			Семестр 3	Семестр 4
Общий объем	**зач. ед.**	8	4	4
	час.	**288**	144	144
Из них:				
Часы аудиторной работы (всего):		**144**	64	64
Лекции		64	32	32
Практические занятия		0	0	0
Лабораторные/практические занятия по подгруппам		64	32	32
Часы внеаудиторной работы, включая самостоятельную работу обучающегося		**160**	80	80
Вид промежуточной аттестации			экзамен	экзамен

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-бальной) системы оценивания:

- отлично: 91-100 баллов из 100;
- хорошо: 76-90 баллов из 100;
- удовлетворительно: 61-75 баллов из 100.

Студент, желающих исправить экзаменационную оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена.

Обучающиеся, не набравшие достаточного количества баллов для оценки, сдают экзамен в период экзаменационной сессии. Форма проведения экзамена – традиционная, по билетам. В билете 2 вопроса.

Для получения оценки «удовлетворительно» ответ студента хотя бы на 1 вопрос из билета, должен раскрывать тему в общем, и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности.

Для получения оценки «хорошо» студент должен ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. При ответе на вопрос, студент может приводить примеры по описываемой теме. Ответ может содержать небольшие недочеты, допускается отсутствие подробного описания отдельных тем, если воспроизведена их суть.

Для получения оценки «отлично» студент должен ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок, сопровождаться примерами. Студент должен уметь отвечать на вопросы, касающиеся детальных характеристик раскрываемых тем.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
Семестр						
1.	История вычислительной техники, поколения и архитектуры ВТ	8	4		4	0
2.	Архитектура и структура ЭВМ	8	4		4	
3.	Основные элементы и периферийные узлы ЭВМ.	8	4		4	0
4.	Представление данных в ЭВМ.	8	4		4	0
5.	Кодирование данных.	8	4		4	
6.	Логические основы функционирования ЭВМ.	4	2		2	0
7.	Основы построения цифровых логических цепей, принципы организации памяти	4	2		2	
8.	Организация микропроцессорной техники.	8	4		4	0
9.	Основы языка ассемблера.	8	4		4	0
	Всего (часов) за семестр	64	32		32	0
Семестр						
10.	Основы операционных и файловых систем семейства Windows.	8	4		4	0
11.	Основы операционных и файловых систем семейства Unix/Linux.	8	4		4	0

12.	Носители и накопители данных. Принципы восстановления данных.	8	4		4	0
13.	Организация и компоненты системной платы ПК. Шины расширения. Интерфейсы.	8	4		4	
14.	Видео и аудио подсистемы.	8	4		4	0
15.	Стандарты электропитания компьютера.	4	2		2	0
16.	Периферийные устройства ввода/вывода. Сканеры, принтеры, коммуникационные устройства.	8	4		4	0
17.	Ноутбуки и современные мобильные платформы.	4	2		2	0
18	Сервера, блэйд-системы, системы хранения данных. Многопроцессорные комплексы.	8	4		4	0
	Всего (часов) за семестр	64	32		32	2
	Итого (часов)	130	64		64	2

4.2. Содержание дисциплины (*модуля*) по темам

1. История вычислительной техники, поколения и архитектуры ВТ.

История создания и развития вычислительной техники, классификация компьютеров, поколения вычислительной техники.

Лабораторная работа 1. Таймлайн развития информационных технологий и вычислительной техники.

Тест 1. Тест по теме История вычислительной техники, поколения и архитектуры ВТ.

2. Архитектура и структура ЭВМ

Архитектура и структура компьютера, принципы Фон Неймана, машина Фон Неймана, Гарвардская архитектура. Измерение производительности компьютера, факторы, влияющие на быстродействие ЭВМ.

Лабораторная работа 3. Работа в эмуляторе машины Фон Неймана.

Тест 2. Тест по теме Архитектура и структура ЭВМ.

3. Основные элементы и периферийные узлы ЭВМ.

Основные компоненты компьютера, их назначение и взаимодействие в системе. Обзор основных периферийных устройств. Обзор технологии создания дисковых массивов. Назначение и возможности интерфейсов, основные интерфейсы ЭВМ.

Тест 3. Тест по теме Основные элементы и периферийные узлы ЭВМ.

4. Представление данных в ЭВМ.

Системы счисления, перевод чисел из одной системы счисления в другую. Представление информации в ЭВМ, методы двоичного кодирования положительных и отрицательных чисел.

Лабораторная работа 4. Перевод чисел между различными системами счисления.

Лабораторная работа 5. Представление данных в ЭВМ.

Тест 4. Тест по теме Представление данных в ЭВМ.

5. Кодирование данных.

Методы кодирования данных. Коды с обнаружением ошибок, коды с исправлением ошибок. Совершенные коды. Циклические коды.

Лабораторная работа 6. Реализация алгоритма кодирования данных.

Тест 5. Тест по теме Кодирование данных.

6. Логические основы функционирования ЭВМ

Основные логические элементы ЭВМ (вентили). Основы алгебры логики. Синтез логических схем, эквивалентность схем, минимизация и приведение к базису. Сумматоры, виды, примеры использования.

Лабораторная работа 7. Применение программного обеспечения для проектирования схем вычислительных устройств.

Лабораторная работа 8. Применение аппарата булевой алгебры для проектирования схем вычислительных устройств.

Тест 6. Тест по теме Логические основы функционирования ЭВМ.

7. Основы построения цифровых логических цепей, принципы организации памяти.

Триггеры. Организация и структура памяти ЭВМ. Элементы памяти, их назначение, возможности и принцип работы.

Лабораторная работа 8. Изучение и анализ триггеров.

Лабораторная работа 9. Принципы организации памяти.

Тест 7. Тест по теме Основы построения цифровых логических цепей, принципы организации памяти.

8. Организация микропроцессорной техники.

Понятие микропроцессора (МП), виды технологии производства МП, поколения МП и их основные характеристики. Обобщенная структура МП, основные промышленные линии микропроцессоров, перспективные МП. Системная магистраль, буферизация шин, управление системной магистралью, подключение дополнительных и интерфейсных схем. Система прерываний. Назначение, принцип работы и организация системы прерываний ЭВМ. Система ввода-вывода.

Тест 8. Тест по теме Организация микропроцессорной техники.

9. **Основы языка Ассемблера**.

Инструментальные средства или что требуется для работы с ассемблером. Использование среды Delphi для изучения языка ассемблера, организация памяти (intel), регистры, непривилегированные команды процессоров Intel серии x86, структура программы на языке ассемблера, простые программы на языке ассемблера.

Лабораторная работа 10. Изучение способов адресации памяти микропроцессором.

Лабораторная работа 11. Основы языка Ассемблера.

Тест 9. Тест по теме Основы языка Ассемблера.

10. Основы операционных и файловых систем семейства Windows.

Операционные системы (ОС) MS DOS, ОС MS Windows. История, особенности современной архитектуры ОС Windows, процесс загрузки/альтернативная загрузка, системный реестр, особенности пользовательских и серверных версий. Стратегия/модель безопасности, работа/настройка политик безопасности, использование сертификатов и подписей в работе ОС. Возможные проблемы и неисправности, методы их устранения.

Лабораторная работа 12. Изучение операционной системы Windows.

Лабораторная работа 13. Изучение файловой системы FAT.

Тест 10. Тест по теме Основы операционных и файловых систем семейства Windows.

11. Основы операционных и файловых систем семейства Unix/Linux.

История появления, версии, особенности современной архитектуры *nix систем. Стратегия/модель безопасности, работа/настройка политик безопасности. Возможные проблемы и неисправности, методы их устранения.

Лабораторная работа 14. Изучение операционной системы Linux.

Тест 11. Тест по теме Основы операционных и файловых систем семейства Unix/Linux.

12. Носители и накопители данных.

Принципы восстановления данных. Дисковая память: назначение, виды, принципы работы и технические характеристики, маркировка. Основные производители, модели, их особенности. Способы подключения (IDE, SATA, SAS). Средства защиты. Технология S.M.A.R.T. Возможные технические проблемы и неисправности, методы их устранения. Восстановление данных. (случаи повреждения и способы восстановления: MBR, таблицы разделов, информации. Общие принципы восстановления данных на носителях информации, обзор ПО). Оптические носители данных. Флэш-носители данных.

Лабораторная работа 15. Изучение RAID массивов в ОС Windows и Linux.

Тест 12. Тест по теме Носители и накопители данных.

13. Организация и компоненты системной платы ПК. Шины расширения. Интерфейсы.

Материнская плата: назначение, компоненты, технические характеристики современных мат. плат, сокеты, маркировка, чипсет, каналы ОЗУ. ПЗУ BIOS/EFI/UEFI: назначение, виды, параметры настройки, способы защиты компьютера, маркировка. Шины расширения (PCI, версии 2/3/64/66/Express, SCSI версии 1/2/Ultra/Fast, SAS и др.) Интерфейсы, шины и разъемы ПК для подключения внешних устройств. (COM, LPT, DeviceBay, PS/2, USB, FireWire и др.) Возможные проблемы и неисправности, методы их устранения.

Лабораторная работа 16. Изучение BIOS.

Тест 13. Тест по теме Организация и компоненты системной платы ПК. Шины расширения. Интерфейсы.

14. Видео и аудио подсистемы.

Видеокарты: назначение, принцип работы, технические характеристики, современные модели/производители, маркировка. Технологии ускорения трехмерной графики. (PhysX, DirectX, OpenGL, Glide). Звуковые карты: назначение, принцип работы, технические характеристики маркировка. Возможные проблемы и неисправности, методы их устранения.

Тест 14. Тест по теме Видео и аудио подсистемы.

15. Стандарты электропитания компьютера.

Виды блоков питания, управление электропитанием (стандарты APM, ACPI, Energy Star). Системы бесперебойного питания. Возможные проблемы и неисправности, методы их устранения. Виды корпусов ПК, системы охлаждения.

Тест 15. Тест по теме Стандарты электропитания компьютера.

16. Периферийные устройства ввода/вывода.

Сканеры, принтеры, коммуникационные устройства. Системы отображения (мониторы/проекторы/альтернативные системы и т.д.): виды, область применения, принцип работы, технические характеристики, маркировка. Способы подключения (vga, dvi, hdma, display port и пр.) Печатающие устройства (принтеры, плоттеры, 3D и пр.): виды, принцип работы, технические характеристики способы подключения. Сканеры и прочие устройства цифрового ввода информации: виды, принцип работы, технические характеристики способы подключения. Возможные проблемы и неисправности, методы их устранения.

Тест 16. Тест по теме Периферийные устройства ввода/вывода.

17. Ноутбуки и современные мобильные платформы.

Ноутбуки: основные характеристики, архитектура, особенности. Возможные проблемы и неисправности, методы их устранения. Мобильные платформы (смартфоны/планшеты): разновидности устройств, основные характеристики, особенности архитектуры, операционные системы.

Тест 17. Тест по теме Ноутбуки и современные мобильные платформы.

18. Сервера, блэйд-системы, системы хранения данных. Многопроцессорные комплексы.

Многопроцессорные комплексы (суперкомпьютеры), сервера для рабочей группы/блэйд-системы. Системы хранения. Распределенные файловые системы (nfs, rfs, GoogleFS и др.), параллельные, симметричные ФС. Понятие кластера. Технологии виртуализации: понятие, основные технологии, обзор основных вендоров и программного обеспечения.

Тест 18. Сервера, блэйд-системы, системы хранения данных. Многопроцессорные комплексы.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
Семестр 3		
1.	История вычислительной техники, поколения и архитектуры ВТ	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Выполнение индивидуального практического задания.
2.	Архитектура и структура ЭВМ	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Выполнение индивидуального практического задания
3.	Основные элементы и периферийные узлы ЭВМ.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Выполнение индивидуального практического задания

4.	Представление данных в ЭВМ.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Выполнение индивидуального практического задания
5.	Кодирование данных.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Выполнение индивидуального практического задания
6.	Логические основы функционирования ЭВМ.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Выполнение индивидуального практического задания
7.	Основы построения цифровых логических цепей, принципы организации памяти	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Выполнение индивидуального практического задания
8	Организация микропроцессорной техники.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Выполнение индивидуального практического задания
9	Основы языка ассемблера.	
Семестр 4		
10.	Основы операционных и файловых систем семейства Windows.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Подготовка доклада.
11.	Основы операционных и файловых систем семейства Unix/Linux.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Подготовка доклада.
12.	Носители и накопители данных. Принципы восстановления данных.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Подготовка доклада.
13.	Организация и компоненты системной платы ПК. Шины расширения. Интерфейсы.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Подготовка доклада.
14.	Видео и аудио подсистемы.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Подготовка доклада.
15.	Стандарты электропитания компьютера.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Подготовка доклада.
16	Периферийные устройства ввода/вывода. Сканеры, принтеры, коммуникационные устройства.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Подготовка доклада.
17	Ноутбуки и современные мобильные платформы.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Подготовка доклада.
18	Сервера, блэйд-системы, системы хранения данных.	Работа с учебной литературой и источниками информации. Подготовка к лабораторным работам и тестированию. Подготовка доклада.

	Многопроцессорные комплексы.	

Порядок выполнения каждого вида самостоятельной работы:

1) Изучение лекционного материала по теме.
2) Изучение основной и дополнительной литературы.
3) Подготовка доклада по теме.
4) Выполнение индивидуального практического задания.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации — экзамен по билетам. Экзамен проводится в виде подготовки студентом письменного ответа на вопросы билета и последующая устная беседа с ответами на вопросы.

Вопросы к экзамену.

Семестр 3.

1. Краткая история развития вычислительной техники (ВТ), разнообразие современных платформ ВТ. Основные понятия и классификация.
2. Микропроцессорная техника, понятие МП, виды технологии производства МП, основные характеристики МП, ретроспективный обзор истории развития микропроцессорной техники.
3. Архитектура и структура ЭВМ. Машина Фон Неймана, гарвардская архитектура.
4. Составные компоненты компьютера, измерение производительности компьютера, факторы, влияющие на быстродействие.
5. Представление чисел в ЭВМ. Разрядная сетка. Двоичные коды. Коды, применяемые для представления отрицательных и вещественных чисел.
6. Кодирование данных. Понятие кодирования, двоично-десятичный код, помехоустойчивое кодирование.
7. Логические принципы функционирования ЭВМ. Элементарные операционные узлы (вентили). Способы задания двоичных функций, эквивалентность схем, минимизация и приведение к базису двоичных функций. Сумматоры.
8. Элементарные операционные узлы ЭВМ. Логические цепи, триггеры, регистры. Организация памяти на триггерах. Способы организации многоразрядных микросхем памяти.
9. Центральный процессор. Структура, принцип работы, режимы работы, системы команд.
10. Микропроцессорная система, как система трёх шин. Определение шины, классификация шин.
11. Организация памяти для микропроцессоров (МП) Intel. Регистры МП x86, виды, назначение.

12. Схема управления прерываниями микропроцессора (МП), схема управления прямым доступом к памяти, режимы процессора, понятие среды выполнения.

Семестр 4.

1. Логическая структура жесткого диска. MBR, разделы, процесс загрузки операционной системы.

2. Файловая система FAT. Основные понятия, версии ФС FAT, ошибки ФС FAT и способы их устранения.

3. ОС Windows. История развития, архитектура, системный реестр, особенности пользовательских и серверных версий, стратегия/модель безопасности. Возможные проблемы и неисправности, методы их устранения.

4. ПЗУ BIOS(MBR)/EFI/UEFI(GPT). Назначение, виды, параметры настройки, способы защиты компьютера, маркировка. Возможные проблемы и неисправности, методы их устранения.

5. Файловая система NTFS (+расширение EFS), WinFS, ReFS.

6. Флэш-память. Назначение, принцип работы, технические характеристики маркировка, средства защиты. Возможные проблемы и неисправности, методы их устранения.

7. ОС UNIX, Linux. История развития, архитектура, стратегия безопасности. Стандарты POSIX, FHS, LSB.

8. Оптические носители (CD, DVD, BD, M-Disc и пр.) Назначение, принцип работы, технические характеристики маркировка, тенденции развития. защита от копирования. Файловые системы оптических носителей.

9. Файловые системы UNIX (s5, ufs, vfs, extX).

10. Звуковые карты. Назначение, принцип работы, технические характеристики маркировка. Возможные проблемы и неисправности, методы их устранения.

11. Современные процессоры. Виды, технические характеристики, ядра, применяемые технологии, маркировка, тенденции развития.

12. Материнская плата. Назначение, компоненты, технические характеристики современных мат. плат, сокеты, маркировка, чипсет, каналы ОЗУ. Возможные проблемы и неисправности, методы их устранения.

13. Видеокарты. Назначение, принцип работы, технические характеристики, современные модели/производители, маркировка. Возможные проблемы и неисправности, методы их устранения.

14. Мобильные платформы (смартфоны, планшеты и пр.). Разновидности устройств, основные характеристики, особенности архитектуры, операционные системы.

15. Шины расширения (PCI, версии 2/3/64/66/Express, SCSI версии 1/2/Ultra/Fast, SAS и др.) Назначение, принцип работы, технические характеристики, особенности, тенденции развития.

16. Интерфейсы, шины и разъемы ПК для подключения внешних устройств. (COM, LPT, DeviceBay, PS/2, USB, FireWire), Принцип работы, технические характеристики маркировка.

17. Оперативная память (технологии DRAM, SRAM, MRAM). Виды системной ОЗУ, назначение, принцип работы, технические характеристики маркировка. Возможные проблемы и неисправности, методы их устранения.

18. Кэширование. Виды кеширования, назначение, принцип работы, технические характеристики кеш-памяти.

19. Электропитание. Виды блоков питания, управление электропитанием (стандарты APM, ACPI, Energy Star). Системы бесперебойного питания. Возможные проблемы и неисправности, методы их устранения. Виды корпусов ПК, системы охлаждения.

20. Печатающие устройства (принтеры, плоттеры, 3D и пр.) Виды, принцип работы, технические характеристики способы подключения. Возможные проблемы и неисправности, методы их устранения.

21. Сканеры. Виды, принцип работы, технические характеристики. Возможные проблемы и неисправности, методы их устранения. Прочие устройства цифрового ввода информации.

22. Дисковая память (HDD). Назначение, виды, принципы работы и технические характеристики, маркировка. Основные производители, модели, их особенности. Способы подключения (IDE, SATA, SAS). Понятие RAID массива. Технология S.M.A.R.T. Возможные технические проблемы и неисправности, методы их устранения.

23. Восстановление данных. Виды нарушений работоспособности и способы восстановления: MBR, таблицы разделов, информации. Общие принципы восстановления данных на носителях информации, обзор программного обеспечения.

24. Ноутбуки. Основные характеристики, особенности архитектуры. Возможные проблемы и неисправности, методы их устранения.

25. Системы отображения. Виды, принцип работы, технические характеристики, маркировка. Способы проводного подключения (vga, dvi, hdma, display port и пр.) Протоколы сетевой передачи мультимедиа (dlna, miracast и пр.). Возможные проблемы и неисправности, методы их устранения.

26. Многопроцессорные комплексы (суперкомпьютеры). Сервера для рабочей группы/Блэйд-системы. Понятие серверного кластера, облачной архитектуры. Системы хранения.

27. Микроконтроллеры. Однокристальные системы.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (из паспорта компетенций)	Оценочные материалы	Критерии оценивания
1.	ОПК-1 способность анализировать физические явления и процессы при решении		Теоретическая часть, Практическая часть	Знает: организацию и структуру центрального процессора, памяти, системы прерывания, системы ввода вывода; организацию системной магистрали, способы

	профессиональных задач			подключения дополнительных устройств; физические основы и принципы действия периферийных устройств, интерфейсы периферийных устройств; Умеет: формализовать поставленную задачу; разбираться в устройстве рабочих станций, ноутбуков, серверов; осуществлять обоснованный выбор стандартного периферийного оборудования; применять полученные знания к различным предметным областям.
2.	ОПК-7 способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения		Теоретическая часть, Практическая часть	Знает: основные этапы создания и развития ЭВМ; существующие виды архитектур ЭВМ, назначение и функции ее элементов; структуру и принципы работы современных и перспективных микропроцессоров; основы языка низкого уровня (язык ассемблера). Умеет: работать с современной элементной базой электронной аппаратуры; определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав параметры периферийных устройств.
3.	ПК-12 способность проводить инструментальный мониторинг защищенности компьютерных систем		Теоретическая часть, Практическая часть	Знает: основы теории кодирования данных; Умеет: осуществлять программную реализацию различных алгоритмов кодирования данных.

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Степина, В. В. Архитектура ЭВМ и вычислительные системы: учебник / В.В. Степина. — Москва: КУРС: ИНФРА-М, 2019. — 384 с. — (Среднее профессиональное образование). - Режим доступа: https://znanium.com/catalog/product/1038451 (дата обращения: 15.05.2020). – заменить на издание для студентов вузов

7.2. Дополнительная литература:

1. Максимов, Н. В. Архитектура ЭВМ и вычислительных систем: учебник / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2020. — 511 с. — (Среднее профессиональное образование). - Режим доступа: https://znanium.com/catalog/product/1079429 (дата обращения: 15.05.2020). - заменить на издание для студентов вузов

2. Зверева, В. П. Технические средства информатизации: учебник / В.П. Зверева, А.В. Назаров. - Москва: КУРС: ИНФРА-М, 2020. - 248 с. - (Среднее профессиональное образование). - Режим доступа: https://znanium.com/catalog/product/1110130 (дата обращения: 15.05.2020). - заменить на издание для студентов вузов

7.3. Интернет-ресурсы

Не предусмотрено

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Программный пакет Microsoft Office,
- Oracle VirtualBox,
- Active@ DiskEditor.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Аудитория с проектором для лекционных занятий; Компьютерный класс с возможностью подключения к сети Интернет для проведения лабораторных занятий.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
“01” июня 2020 г.

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Зулькарнеев И.Р. Программно-аппаратные средства обеспечения информационной безопасности. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» опубликована на сайте ТюмГУ: Программно-аппаратные средства обеспечения информационной безопасности [электронный ресурс] / Режим доступа: https://www.utmn.ru/sveden/education/#

© Тюменский государственный университет, 2020.
© Зулькарнеев И.Р., 2020.

1. Пояснительная записка

Учебная дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» является теоретическая и практическая подготовка работе с современными отечественными средствами защиты информации и внедрение их в систему защиты информации.

Для достижения поставленной цели предусмотрены следующие задачи:

- изучить типы и виды средств защиты информации;
- дать представление о существующих отечественных и зарубежных средствах защиты информации;
- научить устанавливать, настраивать и администрировать средства защиты информации;
- научить делать обоснованный выбор средства защиты информации при проектировании системы защиты информации.

1.1. Место дисциплины (модуля) в структуре образовательной программы

Данная дисциплина входит в блок Б1, Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Организация электронно-вычислительных машин и вычислительных систем», «Администрирование операционных систем».

Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» преподается в 7-8 семестрах, обеспечиваемых дисциплин нет, вырабатываемые компетенции обеспечивают выполнение выпускной квалификационной работы.

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (модуля)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-8: способность к самоорганизации и самообразованию		Знать: дополнительные источники получения информации по администрированию средств защиты; Уметь: находить необходимую дополнительную информацию по средству защиты на сайте компании-производителя;
ПК-5: способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы,		Знать: подходы к сертификации и безопасной разработке средств защиты информации; Уметь: осуществлять подбор необходимых технологий при разработке средств защиты информации;

системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		
ПК-18: способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		Знать: основные угрозы безопасности информации; требования к обеспечению ИБ различными техническими мерами; принципы работы и основной функционал средств защиты информации; Уметь: сопоставлять реализуемый средствами защиты информации функционал с предъявляемыми требованиями по ИБ; определять нейтрализуемые средствами защиты информации угрозы; формулировать требования к конфигурированию средств защиты информации;
ПК-20: способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций		Знать: основные модули и функциональные возможности средств защиты информации; требования к среде функционирования средства защиты информации; Уметь: проводить проверку работоспособности средств защиты информации

* не предусмотрено

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Часов в семестре**	
			9 семестр	10 семестр
Общая трудоемкость	**зач. ед.**	**8**	**4**	**4**
	час	**288**	**144**	**144**
Из них:				
Часы аудиторной работы (всего):		**144**	**72**	**72**
Лекции		64	32	32
Практические занятия		64	32	32

Лабораторные / практические занятия по подгруппам	0	0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	**160**	**80**	**80**
Вид промежуточной аттестации (экзамен)		Зачет	Экзамен

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной) и традиционной (5-балльной) систем оценок.

В 9 семестре по данной дисциплине предусмотрен зачет. Оценка за зачет студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время лабораторных работ, индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины. Для получения зачета необходимо набрать не менее 61 балла. Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать зачет.

В 10 семестре предусмотрен экзамен. Экзаменационная оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время лабораторных работ, индивидуальных домашних заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

- 61 - 76 баллов - удовлетворительно;
- 77 - 90 баллов - хорошо;
- 91 -100 баллов - отлично.;

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете 2 теоретических вопроса. Для получения оценки «удовлетворительно» студентом должно быть сдано минимум 80% практических работ и сделан ответ на 2 вопроса из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы, и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен сдать минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен детально раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы, и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен сдать все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами.

Примечание. Студент, желающий исправить экзаменационную оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена.

Баллы проставляются за посещение лекционных и практических занятий и активную работу на них, а также за выполненные лабораторных работы по каждой теме дисциплины.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№		Объем дисциплины (модуля), час

	Наименование тем и/или разделов	Всего	Виды аудиторной работы (в час)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные / практические занятия по подгруппам	
1	2	3	4	5	6	7
Семестр 9						
1.	Классификация и виды средств защиты информации	24	8	6	0	
2.	Система сертификации средства защиты информации в РФ	16	6	0	0	
3.	Средства доверенной загрузки	20	6	4	0	
4.	Средства защиты от несанкционированного доступа	84	12	22	0	
	Всего (часов) за 7 семестр	144	32	32	0	0
Семестр 10						
5.	Средства криптографической защиты информации	96	20	20	0	
6.	Средства антивирусной защиты	12	4	2	0	
7.	Средства анализа и контроля защищенности	12	4	2	0	
8.	Выбор технических мер при проектировании системы защиты информации	24	4	8	0	
	Всего (часов) за 8 семестр	144	32	32	0	2
	Итого (часов)	288	64	64	0	2

4.2. Содержание дисциплины *(модуля)* по темам

Семестр 7.

Классификация и виды средств защиты информации

Понятие средства защиты информации. Классификация средств защиты информации. Виды средства защиты информации. Отечественные и зарубежные средства защиты информации.

Практическая работа 1.

Подготовить доклад и презентацию, посвященную определенному виду средств защиты информации.

Система сертификации средства защиты информации в РФ

Понятие оценки соответствия требованиям защиты информации. Формы и виды. Процедура сертификации средств защиты информации. Требования, предъявляемые к компании-заявителю. Формы проведения сертификации. Виды сертифицируемых средств защиты информации и требования, предъявляемые к ним.

Средства доверенной загрузки

Понятие средств доверенной загрузки. Основной функционал и варианты установки и настройки. Варианты применения в зависимости от требований по информационной безопасности. Средство доверенной загрузки «Соболь».

Практическая работа 2.

Установка средства доверенной загрузки «Соболь». Настройка в соответствии с требованиями безопасности. Проверка работоспособности каждого модуля.

Средства защиты от несанкционированного доступа

Понятие средств защиты от НСД. Основной функционал и варианты установки и настройки. Варианты применения в зависимости от требований по информационной безопасности. Средство защиты от НСД «Secret Net Studio».

Практическая работа 3.

Установка средств защиты от НСД «Secret Net Studio». Настройка в соответствии с требованиями безопасности. Проверка работоспособности каждого модуля. Работа с методическим лабораторным практикумом.

Семестр 8.

Средства криптографической защиты информации

Понятие СКЗИ. Основной функционал и варианты установки и настройки. Варианты применения в зависимости от требований по информационной безопасности. СКЗИ «ViPNet».

Практическая работа 4.

Установка СКЗИ «ViPNet». Настройка в соответствии с требованиями безопасности. Проверка работоспособности каждого модуля. Работа с методическим лабораторным практикумом.

Средства антивирусной защиты

Понятие средств антивирусной защиты. Основной функционал и варианты установки и настройки. Варианты применения в зависимости от требований по информационной безопасности.

Практическая работа 5.

Установка средства антивирусной защиты. Настройка в соответствии с требованиями безопасности. Проверка работоспособности каждого модуля.

Средства анализа и контроля защищенности

Понятие средства анализа и контроля защищенности. Основной функционал и варианты установки и настройки. Варианты применения в зависимости от требований по информационной безопасности.

Практическая работа 6.

Установка средства анализа и контроля защищенности. Настройка в соответствии с требованиями безопасности. Проверка работоспособности каждого модуля.

Выбор технических мер при проектировании системы защиты информации

Правила выбора средств защиты информации в зависимости от предъявляемых требований безопасности и классов информационных систем. Варианты внедрения средств защиты информации в систему защиты информации на этапе ее проектирования. Принципы сравнения средств защиты информации одного вида.

Практическая работа 7.

Подготовка проекта внедрения средств защиты информации для определенной информационной системы.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ Темы	Темы	Формы СРС, включая требования к подготовке к занятиям
Семестр 9		
1.	Классификация и виды средств защиты информации	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам
2.	Система сертификации средства защиты информации в РФ	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам
3.	Средства доверенной загрузки	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам
4.	Средства защиты от несанкционированного доступа	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам
Семестр 10		
5.	Средства криптографической защиты информации	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам
6.	Средства антивирусной защиты	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам
7.	Средства анализа и контроля защищенности	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам
8.	Выбор технических мер при проектировании системы защиты информации	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение основной и дополнительной литературы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1 Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации – зачет (7 семестр) и экзамен (8 семестры). Зачет и экзамен проходят в традиционной форме, по билетам. В билете – 2 теоретических вопроса.

Вопросы к зачету:

9 семестр

1. Методы и средства защиты информации. Определения и примеры.
2. Развернутое определение СрЗИ. Классификации СрЗИ с примерами.
3. Оценка соответствия СрЗИ требованиям по безопасности информации. Понятие. Формы.
4. Порядок сертификации СрЗИ по требованиям ФСТЭК России.
5. Виды сертификации СрЗИ. Отличия ЗБ от ТУ.
6. Архитектура и состав Secret Net Studio. Реализация 5-уровневой защиты
7. Функционал защиты Secret Net Studio для защиты уровня данных.
8. Функционал защиты Secret Net Studio для защиты уровня приложений.
9. Функционал защиты Secret Net Studio для защиты уровня сети.
10. Функционал защиты Secret Net Studio для защиты уровня операционной системы.
11. Функционал защиты Secret Net Studio для защиты уровня периферийного оборудования.
12. Режимы работы Secret Net Studio.
13. Архитектура и состав ПАК «Соболь».
14. Функциональные возможности ПАК «Соболь».

10 семестр

1. Основы построения виртуальных частных сетей VPN (назначение, классификация, туннелирование, инкапсуляция)
2. Виртуальные защищенные сети ViPNet (назначение, отличительные особенности, инкапсуляция в ViPNet, поддерживаемые ОС)
3. Состав и назначение комплекса ViPNet Custom. Используемые в данном комплексе технологии защиты информации
4. Состав и основные функции ViPNet Администратор
5. Состав и основные функции ViPNet Координатор
6. Состав и основные функции ViPNet Клиент
7. Теоретическая проработка схемы защищенной сети (построение сетевой и прикладной структуры защищенной сети)
8. Основные понятия сети ViPNet (основные понятия адресной администрации, основные понятия прикладной администрации, идентификации объектов защищенной сети)
9. Особенности криптосистемы ViPNet Криптоядро «Домен-К»
10. Используемые в ViPNet алгоритмы шифрования, хеширования, ЭЦП. Схема открытого распространения симметричных ключей Диффи-Хелмана. Комбинация криптографических алгоритмов с симметричными и ассиметричными ключами
11. Типы ключей, используемых в ViPNet и схемы их формирования
12. Защита ключевой информации в ViPNet (ключи защиты, схемы защиты ключевой информации)
13. Состав ключевой информации пользователя (общий ключевой набор, индивидуальный ключевой набор, полный и минимальный дистрибутив)

14. Электронная цифровая подпись в технологии ViPNet (Основные определения, назначение, состав программного комплекса УЦ ViPNet, общая технология УЦ)
15. Классификации АС по защите от НСД. Классификация по уровню контроля отсутствия НДВ. Классификация защищенности СВТ
16. Классификация средств антивирусной защиты
17. Классификация средств анализа и контроля защищенности

6.2 Критерии оценивания компетенций:

Таблица 4

Карта критериев оценивания компетенций

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОК-8: способность к самоорганизации и самообразованию	Знать: дополнительные источники получения информации по администрированию средств защиты; Уметь: находить необходимую дополнительную информацию по средству защиты на сайте компании-производителя;	Практическая работа. Зачет Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-5: способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты	Знать: подходы к сертификации и безопасной разработке средств защиты информации; Уметь: осуществлять подбор необходимых технологий при	Практическая работа. Зачет Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические

	информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	разработке средств защиты информации;		вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
3.	ПК-18: способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать: основные угрозы безопасности информации; требования к обеспечению ИБ различными техническими мерами; принципы работы и основной функционал средств защиты информации; Уметь: сопоставлять реализуемый средствами защиты информации функционал с предъявляемыми требованиями по ИБ; определять нейтрализуемые средствами защиты информации угрозы; формулировать требования к конфигурированию средств защиты информации;	Практическая работа. Зачет Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

4.	ПК-20: способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	Знать: основные модули и функциональные возможности средств защиты информации; требования к среде функционирования средства защиты информации; Уметь: проводить проверку работоспособности средств защиты информации	Практическая работа. Зачет Экзамен.	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература:

1. Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2017. - 198 с.: ISBN 978-5-4446-1043-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/977192 (дата обращения: 20.05.2020). – Режим доступа: по подписке. **Такое же описание в Дополнительной. Прошу заменить на:** Аппаратные и программные средства защиты информации: Учебное пособие / Душкин А.В., Кольцов А., Кравченко А. - Воронеж:Научная книга, 2016. - 232 с. ISBN 978-5-4446-0746-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/923168 (дата обращения: 20.05.2020). – Режим доступа: по подписке.

7.2 Дополнительная литература:

1. Хорев, П. Б. Программно-аппаратная защита информации : учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). - ISBN 978-5-00091-709-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1025261 (дата обращения: 20.05.2020). – Режим доступа: по подписке.
2. Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2017. - 198 с.: ISBN 978-5-4446-1043-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/977192

(дата обращения: 20.05.2020). – Режим доступа: по подписке.

7.3 Интернет-ресурсы:

1. https://fstec.ru/
2. сайты компаний-производителей средств защиты информации

7.4 Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) https://icdlib.nspu.ru/
- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА https://rusneb.ru/
- Справочная правовая система КонсультантПлюс http://www.consultant.ru/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю):

- программное обеспечение виртуализации: VMWare, VirtualBox или другое
- операционная система Windows 7 или более поздние версии
- установленное ПО: MS Office
- платформа для электронного обучения Microsoft Teams

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Аудитория с проектором; ПК с установленным ПО: MS Office.

Компьютерный класс с не менее 15 ПК.

Специализированная лаборатория программно-аппаратных средств обеспечения информационной безопасности, оснащенная следующими техническими средствами и программным обеспечением:

– Программно-аппаратный комплекс СДЗ Соболь (4 комплекта).

— ПО ViPNet Custom в составе:

ПО ViPNet Administrator 4.x, 2 шт
ПО ViPNet Coordinator Windows 4.x, 2 шт
ПО ViPNet Coordinator Linux, 2 шт
ПО ViPNet Client 4.x, 30 шт
ПО ViPNet Registration Point 4.x, 2 шт
ПО ViPNet Publication Service 4.x, 2 шт
ПО ViPNet ЭП внешние, 100 шт
ПО ViPNet ЭП внутренние, 100 шт
ПО ViPNet StateWatcher 4.x, 2 шт
ПО ViPNet StateWatcher на 1 узел мониторинга, 30 шт
ПО ViPNet Policy Manager 4.x, 2 шт
ПО ViPNet Policy Manager на 1 узел управления, 30 шт

— Виртуальный программно-аппаратный комплекс ViPNet Coordinator HW1000 (Virtual Applince), 2 шт

— Виртуальный программно-аппаратный комплекс ViPNet Coordinator HW1000 IDS (Virtual Applince), 1 шт,

— Программное обеспечение Positive Technologies Application Firewall Education (10 лицензий),

— Программное обеспечение MaxPatrol Education (1 лицензия),

— Программное обеспечение XSpider Education (10 лицензий),

— Электронный USB-ключ SafeNet eToken и ПО для взаимодействия с ключем (4 комплекта).
— Программное обеспечение InfoWatch Traffic Monitor Enterprise Edition, 50 лицензий, договор
— Средство защиты информации Secret Net Studio 8, 10 шт,
— Средство защиты информации Secret Net 7. Клиент (автономный режим работы), 5 шт,
— Средство защиты информации Secret Net 7. Сервер безопасности класса С, 1 шт,
— Средство защиты информации Secret Net 7. Клиент (сетевой режим работы, 10 шт,
— Средство защиты информации Secret Net LSP, 10 шт,
— ПО Континент АП, 10 шт,
— Сервер авторизации ПО vGate R2, 1 шт,
— Резервный Сервера авторизации ПО vGate R2, 1 шт,
— ПО vGate R2 для защиты ESX-хостов, 2 шт,
— Сервера авторизации ПО vGate для Hyper-V, 1 шт,
— Резервный Сервер авторизации ПО vGate для Hyper-V, 1 шт,
— ПО vGate для Hyper-V для защиты хостов, 2 шт,

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
“01” июня 2020 г.

СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ
Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Оленников А.А. Системы видеонаблюдения. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Системы видеонаблюдения [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Оленников А.А., 2020.

1. Пояснительная записка

Учебная дисциплина «Системы видеонаблюдения» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Целью дисциплины «Системы видеонаблюдения» является обучение студентов основам проектирования систем видеонаблюдения, ознакомиться с современным оборудованием, изучить методики расчета и подбора оборудования, изучить технологические схемы, используемые в сблокировке с охранно-пожарными и другими системами.

Задачи дисциплины «Системы видеонаблюдения»:

- изучить основную нормативно-техническую документацию;
- изучить основные принципы и подходы при организации технической защиты информации;
- изучить методики расчета и подбора оборудования видеонаблюдения;
- изучить архитектуру сетей видеонаблюдения;
- изучить некоторое сервисное программное обеспечение.
- изучить принципы и подходы к проектированию систем видеонаблюдения.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в базовую часть цикла естественно - научных дисциплин, блок Б1. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Сети и системы передачи информации», «Безопасность сетевых технологий», «Интернет вещей».

Дисциплина «Системы видеонаблюдения» способствует освоению дисциплины: «Защита корпоративных систем», «Безопасность распределенных компьютерных систем».

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-8 – способностью к самоорганизации и самообразованию	----------	**Знать:** Нормативно-техническую документацию; принцип работы оборудования видеонаблюдения; основные подходы к проектированию систем видеонаблюдения. **Уметь:** Ориентироваться в нормативно-технической документации; разрабатывать и применять технические решения для объектов любой сложности; настраивать основное и вспомогательное оборудование.

ПК-14 - способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа.	----------	**Знать:** Методы построения сетей систем видеонаблюдения; типовые схемы систем видеонаблюдения, применяемые на объектах любой сложности; основные подходы к организации защиты сетей видеонаблюдения; способы настройки сетевого оборудования и его мониторинга. **Уметь:** проектировать схемы сетей видеонаблюдения на планах здания; разрабатывать структурные электрические схемы; компоновать телекоммуникационные шкафы и стойки; настраивать сетевое оборудование видеонаблюдения, в том числе межсетевые экраны, программируемые коммутаторы, а также программное обеспечение отвечающее за безопасность сетей видеонаблюдения.

* не предусмотрено

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		9 семестр
Общий объем зач. ед.	4	4
час.	144	144
Из них:		
Часы аудиторной работы (всего):	64	64
Лекции	32	32
Практические занятия	0	0
Лабораторные/практические занятия по подгруппам	32	32
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	80	80
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет

3. Система оценивания

3.1. Текущий и промежуточный контроль освоения и усвоения материала дисциплины осуществляется в рамках модульно-рейтинговой (100-балльной) и традиционной (5-балльной) систем оценок.

Количество баллов, необходимые для получения зачета является интегрированной оценкой выполнения студентом заданий во время лабораторных работ, индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины.

Для получения зачета необходимо набрать не менее 75 баллов.

Студент, у которого сумма набранных баллов, оказалась меньше 75, должен обязательно выполнить и сдать все лабораторные работы и индивидуальные задания, а также подготовить ответы на вопросы, предложенные преподавателем.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «зачтено» студентом должны быть сданы все лабораторные работы и индивидуальные задания, выдаваемые преподавателем в ходе семестра. В зависимости от качества выполненного задания за каждую работу может назначаться разное количество баллов. Изначально предусмотрено, если студент в ходе обучения выполняет в срок лабораторные и индивидуальные задания, посещает лекции и активно работает на них – он автоматически набирает необходимое количество баллов для получения зачета.

Если студент выполняет лабораторные и индивидуальные задания в срок, посещает лекции и активно работает на них, но качество лабораторных работ и индивидуальных заданий неудовлетворительное – обучающийся имеет право доработать лабораторные работы или индивидуальные задания, либо подготовить ответы на вопросы преподавателя.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Введение. Назначение систем видеонаблюдения и их роль. Действующая нормативная документация. Федеральные законы.	10	2	0	2	0
2.	Знакомство со средой автоматизированного проектирования AutoCad.	16	4	0	2	0
3.	Знакомство и изучение реальных проектов и их технических решений.	8	2	0	2	0
4.	Классификация систем видеонаблюдения. Общие требования, предъявляемые к системам	8	2	0	0	0

	видеонаблюдения.					
5.	Виды видеокамер и их устройство. Интерфейсы. Способы настройки и управления. Правила подбора. Датчики сблокированные с камерами.	16	2	0	6	0
6.	Виды объективов для видеокамер. Методика расчета и подбор.	10	2	0	2	0
7.	Инфракрасные прожекторы, их расчет и подбор.	4	2	0	0	0
8.	Кожухи и корпуса видеокамер камер. Обеспечение микроклимата. Методика расчета и подбор.	4	2	0	0	0
9.	Виды видеорегистраторов. Правила подбора. Настройка.	16	2	0	4	0
10.	Делитель экрана. Мультиплексор. Платы видеозахвата.	8	2	0	0	0
11.	Сетевое оборудование для систем видеонаблюдения. Правила подбора. Расчет пропускной способности каналов.	12	2	0	4	0
12.	Источники резервированного питания. Методика подбора. Расчет общей нагрузки. Привязка оборудования к индивидуальному или к центральном источнику питания.	8	2	0	2	0
13.	Оборудование АРМ. Пульты управления. Программные средства регистрации видеосигнала.	8	2	0	2	0
14.	Типовые схемы видеонаблюдения. Простейшие схемы с одним видеорегистратором. Сложные схемы. Схемы, комбинированные с охранно-пожарной сигнализацией, системой СКУД и климатическим	16	4	0	6	0

	оборудованием.					
	Итого (часов)	144	32	0	32	0

4.2. Содержание дисциплины (*модуля*) по темам

Тема 1. Введение. Назначение систем видеонаблюдения и их роль. Действующая нормативная документация. Федеральные законы.

Лабораторная работа 1.

Знакомство с нормативной документацией и составления набора нормативных документов для предложенного объекта.

Тема 2. Знакомство со средой автоматизированного проектирования AutoCad.

Лабораторная работа 2.

Изучение среды автоматизированного проектирования AutoCad. Подготовка рабочей среды и доработка чертежей предложенных объектов для последующей разработки проекта.

Тема 3. Знакомство и изучение реальных проектов и их технических решений.

Лабораторная работа 3.

Подготовка условных обозначений для разрабатываемого проекта.

Тема 4. Классификация систем видеонаблюдения. Общие требования, предъявляемые к системам видеонаблюдения.

Тема 5. Виды видеокамер и их устройство. Интерфейсы. Способы настройки и управления. Правила подбора. Датчики, сблокированные с камерами.

Лабораторная работа 4.

Изучение принципа работы аналоговых и цифровых камер, и их настройка.

Лабораторная работа 5.

Подбор видеокамер для разрабатываемого проекта. Построение зон охвата видеокмерами.

Тема 6. Виды объективов для видеокамер. Методика расчета и подбор.

Лабораторная работа 6.

Расчет фокусного расстояния камер, расчет угла обзора.

Тема 7. Инфракрасные прожекторы, их расчет и подбор.

Тема 8. Кожухи и корпуса видеокамер камер. Обеспечение микроклимата. Методика расчета и подбор.

Тема 9. Виды видеорегистраторов. Правила подбора. Настройка.

Лабораторная работа 7.

Работа с видеорегистратором. Настройка и управление.

Тема 10. Делитель экрана. Мультиплексор. Платы видеозахвата.

Тема 11. Сетевое оборудование для систем видеонаблюдения. Правила подбора. Расчет пропускной способности каналов.

Лабораторная работа 8.

Построение сети для разрабатываемого проекта и расчет пропускной способности каналов и сетевого оборудования.

Тема 12. Источники резервированного питания. Методика подбора. Расчет общей нагрузки. Привязка оборудования к индивидуальному или к центральному источнику питания.

Лабораторная работа 9.

Расчет источника резервированного питания, подбор аккумуляторов.

Тема 13. Оборудование АРМ. Пульты управления. Программные средства регистрации видеосигнала.

Лабораторная работа 10.

Построение структурной электрической схемы для автоматизированного рабочего места.

Тема 14. Типовые схемы видеонаблюдения. Простейшие схемы с одним видеорегистратором. Сложные схемы. Схемы, комбинированные с охранно-пожарной сигнализацией, системой СКУД и климатическим оборудованием.

Лабораторная работа 11.

Разработка структурной электрической схемы для проекта и сблокировка с охранно-пожарными системами и СКУД.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Введение. Назначение систем видеонаблюдения и их роль. Действующая нормативная документация. Федеральные законы.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.
2.	Знакомство со средой автоматизированного проектирования AutoCad.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.
3.	Знакомство и изучение реальных проектов и их технических решений.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.
4.	Классификация систем видеонаблюдения. Общие требования, предъявляемые к системам видеонаблюдения.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.
5.	Виды видеокамер и их устройство. Интерфейсы. Способы настройки и управления. Правила подбора. Датчики сблокированные с камерами.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.
6.	Виды объективов для видеокамер. Методика расчета и подбор.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.
7.	Инфракрасные прожекторы, их расчет и подбор.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.
8.	Кожухи и корпуса видеокамер камер. Обеспечение микроклимата. Методика расчета и подбор.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.
9.	Виды видеорегистраторов. Правила подбора. Настройка.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.
10.	Делитель экрана. Мультиплексор. Платы видеозахвата.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.
11.	Сетевое оборудование для систем видеонаблюдения. Правила подбора. Расчет пропускной способности каналов.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.

12.	Источники резервированного питания. Методика подбора. Расчет общей нагрузки. Привязка оборудования к индивидуальному или к центральном источнику питания.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.
13.	Оборудование АРМ. Пульты управления. Программные средства регистрации видеосигнала.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.
14.	Типовые схемы видеонаблюдения. Простейшие схемы с одним видеорегистратором. Сложные схемы. Схемы, комбинированные с охранно-пожарной сигнализацией, системой СКУД и климатическим оборудованием.	Чтение обязательной и дополнительной литературы, подготовка к лабораторным работам.

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение рекомендованной основной и дополнительной литературы.
3. Выполнение лабораторной работы
4. Защита лабораторной работы с объяснениями

Контроль за самостоятельной работой осуществляется при выполнении обучающимся лабораторной работы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации – зачет. Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса.

Вопросы к зачету.

1. Разработка чертежей стадий П и Р в программном комплексе AutoCad.
2. Основной инструментарий AutoCad.
3. Основные правила 87-го постановления правительства РФ.
4. Состав чертежей и их последовательность.
5. Подготовка рабочего пространства среды AutoCad.
6. Знакомство с основными инструментами среды AutoCad.
7. Разработка рабочих листов требуемого формата в среде AutoCad.
8. Использование библиотек готовых схем и узлов.
9. Проработка планов чертежей объекта.
10. Разработка монтажных схем оборудования.
11. Разработка структурных и принципиальных схем видеонаблюдения.
12. Составление кабельного журнала.

13. Формирование листов спецификации.
14. Составление пояснительной записки к проекту.
15. Правила оформления пояснительной записки.
16. Изучение основных разделов пояснительной записки.
17. Особенности формирования разделов, содержащих техническое решение.
18. Действующая нормативная документация и федеральный законы.
19. Своды правил, ГОСТы, ведомственные строительные нормы в области видеонаблюдения.
20. Общие требования, предъявляемые к системам видеонаблюдения.
21. Оборудование для систем видеонаблюдения.
22. Видеокамеры аналоговые и цифровые.
23. Устройство телевизионной камеры.
24. Видеодетектор движения.
25. Кожухи и корпуса камер.
26. Термокожухи.
27. Устройство поворотное и наклона видеокамеры.
28. Инфракрасная подсветка и прожекторы.
29. Виды объективов и их подбор.
30. Видеорегистраторы.
31. Делитель экрана. Мультиплексор.
32. Платы видеозахвата.
33. Источники резервированного питания.
34. Средства синхронизации (привязка оборудования к одному источнику питания).
35. Оборудование АРМ. Пульты управления. Программные средства регистрации видеосигнала.
36. Типовые схемы видеонаблюдения. Простейшие схемы с одним видеорегистратором. Схемы комбинированные с охранно-пожарной сигнализацией, системой СКУД и климатическим оборудованием.
37. Подбор подходящего вида камер исходя из плана объекта и его назначения. Методика расчета и подбора камер видеонаблюдения. Расчет и подбор объективов для камер.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОК-8 – способностью к самоорганизации и самообразованию	**Знать:** Нормативно-техническую документацию; принцип работы оборудования видеонаблюдения; основные подходы к проектированию систем видеонаблюдения. **Уметь:** Ориентироваться в нормативно-технической документации; разрабатывать и применять технические решения для объектов любой сложности; настраивать	Собеседование, лабораторные работы, билеты к зачету.	Компетенции сформированы при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных

		основное и вспомогательное оборудование.		заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-14 - способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа.	**Знать:** Методы построения сетей систем видеонаблюдения; типовые схемы систем видеонаблюдения, применяемые на объектах любой сложности; основные подходы к организации защиты сетей видеонаблюдения; способы настройки сетевого оборудования и его мониторинга. **Уметь:** проектировать схемы сетей видеонаблюдения на планах здания; разрабатывать структурные электрические схемы; компоновать телекоммуникационные шкафы и стойки; настраивать сетевое оборудование видеонаблюдения, в том числе межсетевые экраны, программируемые коммутаторы, а также программное обеспечение отвечающее за безопасность сетей видеонаблюдения.	Собеседование, лабораторные работы, билеты к зачету.	Компетенции сформированы при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Бабкин, А, А. Инженерно-технические средства охраны и надзора : учебное пособие для специальности 40.05.02 «Правоохранительная деятельность» и направления подготовки 40.03.01 «Юриспруденция» / А. А. Бабкин ; Федер. служба исполн. наказаний, Вологод. ин-т права и экономики. - Вологда : ВИПЭ ФСИН, 2018. - 143 с. - ISBN 978-5-94991-433-5. - Текст : электронный. - URL:

https://znanium.com/catalog/product/1229047 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

7.2. Дополнительная литература:

1. Землянухин, П. А. Видео- и радиосигналы в системах передачи информации : учебное пособие / П.А. Землянухин ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2017. - 119 с. - ISBN 978-5-9275-2394-8.1020577. - Текст : электронный. - URL: https://znanium.com/catalog/product/1021541 (дата обращения: 15.05.2020). – Режим доступа: по подписке.
2. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2017. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380. - ISBN 978-5-369-01450-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/763644 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

7.3. Интернет-ресурсы

1. Научная электронная библиотека. URL: http://elibrary.ru/.
2. Электронные ресурсы ИБЦ ТюмГУ. URL: https://bmk.utmn.ru/ru/.

7.4 Современные профессиональные базы данных и информационные справочные системы

- Межвузовская электронная библиотека (МЭБ). - URL: https://icdlib.nspu.ru/
- Национальная электронная библиотека. - URL: https://rusneb.ru/
- Institute of Electrical and Electronics Engineers, Inc (IEEE). - URL: https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- Orbit Intelligence. - URL: https://www.orbit.com

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Лицензионное ПО:
  - Microsoft Imagine Academy (ранее Dreamspark): ОС семейства MS Windows (редакция Pro/Server);
  - Офисный пакет Microsoft Office 365 (лицензионное соглашение №2т/00509-20 от 12.05.2020);
  - Платформа для электронного обучения Microsoft Teams.

- Свободно распространяемое ПО:
  - Программное обеспечение виртуализации: VirtualBox (бесплатная лицензия доступна: https://www.virtualbox.org/wiki/Downloads).

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения лекций и лабораторных занятий;

Лаборатории, оснащенные лабораторным оборудованием в соответствии с ФГОС ВО 3+ по данному направлению.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
“01” июня 2020 г.

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Рабочая программа для
обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Паюсова Т.И. Управление информационной безопасностью. Рабочая программа для обучающихся по специальности 10.05.01 Компьютерная безопасность, специализация «Безопасность распределенных компьютерных систем, форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Управление информационной безопасностью [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Паюсова Т.И., 2020.

1. Пояснительная записка

Целью дисциплины «Управление информационной безопасностью» - изучение методов и средств управления информационной безопасностью (ИБ) на объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта (СУИБ).

Задачи курса - изучение:

- Формирование требований к системе управления ИБ конкретного объекта.
- Проектирование системы управления ИБ конкретного объекта.
- Эффективное управление ИБ конкретного объекта.

В результате освоения дисциплины у студентов будут сформированы следующие компетенции:

ОК-8 - способность к самоорганизации и самообразованию;

ПК-7 - способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем;

ПК-13 - способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности;

ПК-15 - способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы.

1.1. Место дисциплины (*модуля*) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Базовая часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Разработка и эксплуатация защищенных автоматизированных систем», «Программноаппаратные средства обеспечения информационной безопасности», «Анализ больших данных», «Разработка защищенных прикладных решений на базе современных систем управления базами данных».

Дисциплина «Управление информационной безопасностью» способствует освоению следующих дисциплин: «Преддипломная практика», «Выпускная квалификационная работа (дипломная работа)».

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (*модуля*)

Код и наименование компетенции	Код и наименование части компетенции*	Компонент (знаниевый/функциональный)
ОК-8 - способность к самоорганизации и самообразованию		Знает: основные принципы построения информационной безопасности; Умеет: использовать современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;

ПК-12 - способность участвовать в проектировании системы управления		Знает: историю информационных технологий; основные направления повышения надежности

информационной безопасностью автоматизированной системы;		вычислительных систем, комплексов и сетей, а также методы и средства обеспечения безопасности и сохранности информации в них; Умеет: понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны; анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ.
ПК-18 - способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности		Знает: основные принципы построения информационной безопасности; Умеет: использовать современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;
ПК-19 - способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы		Знает: основные стандарты, регламентирующие управление ИБ; способы защиты информации в различных операционных системах; Умеет: практически решать задачи формализации разрабатываемых процессов управления ИБ; выделять основные методы организации информационной безопасности в условиях конкретной задачи;

ПК-28 - способность управлять информационной безопасностью автоматизированной системы		Знает: основные стандарты, регламентирующие управление ИБ; принципы разработки процессов управления ИБ; Умеет: определять цели и задачи, решаемые
		разрабатываемыми процессами управления ИБ; анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ.

* не предусмотрено

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	**Всего часов** (академические часы)	**Часов в семестре** (академические часы)
		9 семестр
Общий объем зач. ед.	4	4
час.	144	144
Из них:		
Часы аудиторной работы (всего):	64	64
Лекции	32	32
Практические занятия	32	32
Лабораторные/практические занятия по подгруппам		
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	80	80
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)	зачет	зачет

3. Система оценивания

3.1. Для текущего контроля применяется 100-балльная система оценивания. Баллы проставляются за посещение лабораторных занятий, а также активную работу на них. Результаты текущего контроля учитываются при промежуточной аттестации. Перевод баллов в зачет осуществляется по следующей шкале: от 61 до 100 баллов – «зачтено». Зачет проходит в устной форме, по билетам. В билете – 2 вопроса. Для получения оценки «зачтено» ответ студента должен показывать, что студент знает и понимает смысл и суть описываемой темы, ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Ответ может содержать небольшие недочеты.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные /практические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Введение. Базовые вопросы управления ИБ. Процессный подход.	8	4	4	0	0
2.	Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ	8	4	4	0	0
3.	Рискология ИБ.	8	4	4	0	0
4.	Основные процессы СУИБ. Обязательная документация СУИБ.	8	4	4	0	0
5.	Эксплуатация и независимый аудит СУИБ.	8	4	4	0	0
6.	Внедрение разработанных процессов. Документ «Положение о применимости».	8	4	4	0	0
7.	Процесс «Управление инцидентами ИБ». Процесс «Обеспечение непрерывности ведения бизнеса».	8	4	4	0	0
8.	Обеспечение соответствия требованиям законодательства РФ.	8	4	4	0	0
	Итого (часов)	144	32	32	0	0

4.2. Содержание дисциплины (*модуля*) по темам

Модуль 1.
Основы управления ИБ.

1. **Введение. Базовые вопросы управления ИБ**. Процессный подход. Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний. Сущность и функции управления.

Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Стандартизация в области построения систем управления.

История развития. Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов.

2. **Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ.** Понятие роли. Использование ролевого принципа в рамках СУИБ. Преимущества использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли). Роль высшего руководства организации в СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.). Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ.

3. **Рискология ИБ.** Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Разработка Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Выбор угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ.

Модуль 2. Основные процессы СУИБ.

4. **Основные процессы СУИБ. Обязательная документация СУИБ.** Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности».

5. **Эксплуатация и независимый аудит СУИБ.** Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации. Модуль 3.Процессы.

6. **Внедрение разработанных процессов. Документ «Положение о применимости**». Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения. Сложности, возникающие при внедрении процессов управления ИБ, и способы их решения. Контроль над внедрением процессов. Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа.

7. **Процесс «Управление инцидентами ИБ. Процесс «Обеспечение непрерывности ведения бизнеса».** Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ. Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.

8. **Обеспечение соответствия требованиям законодательства РФ**. Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.). Разработка процессов

или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

Темы лабораторных работ (Лабораторный практикум).

Модуль 1. Основы управления ИБ.

Тема 1. Введение. Базовые вопросы управления ИБ. Процессный подход.

1. Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO/IEC 2700x) **Тема 2. Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ.**
2. Разработка и управление политикой ИБ информационной системы.

Тема 3. Рискология ИБ.

3. Анализ модели угроз ИБ и уязвимостей.
4. Анализ модели информационных потоков.

Модуль 2. Основные процессы СУИБ.

Тема 4. Основные процессы СУИБ. Обязательная документация СУИБ.

5. Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»).
6. Процесс «Анализ со стороны высшего руководства».
7. Процесс «Обучение и обеспечение осведомленности». **Тема 5. Эксплуатация и независимый аудит СУИБ.**
8. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001.
9. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита.

Модуль 3. Процессы.

Тема 6. Внедрение разработанных процессов. Документ «Положение о применимости».

10. Документирование процесса внедрения разработанных процессов.
11. Типовой документ «Положение о применимости».
12. Процесс разработки документа, решение спорных ситуаций при разработке документа.

Тема 7. Процесс «Управление инцидентами ИБ». Процесс «Обеспечение непрерывности ведения бизнеса».

13. Участники процесса. Обязательные этапы процесса.
14. Связи с другими процессами СУИБ.

Тема 8. Обеспечение соответствия требованиям законодательства РФ.

15. Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Введение. Базовые вопросы управления ИБ. Процессный подход.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы, подготовка к устному ответу.

2.	Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ.	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы, подготовка к устному ответу.
3.	Рискология ИБ.	Конспектирование материала на лекционных занятиях. Подготовка к ответу на коллоквиуме. Работа с учебной литературой. Выполнение лабораторной работы.
4.	Основные процессы СУИБ. Обязательная документация	Конспектирование материала на лекционных занятиях. Работа с учебной литературой.
	СУИБ.	Выполнение лабораторной работы, подготовка к устному ответу.
5.	Эксплуатация и независимый аудит СУИБ.	Конспектирование материала на лекционных занятиях. Подготовка к ответу на коллоквиуме. Работа с учебной литературой. Выполнение лабораторной работы, подготовка к устному ответу.
6.	Внедрение разработанных процессов. Документ «Положение о применимости».	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы, подготовка к устному ответу.
7.	Процесс «Управление инцидентами ИБ. Процесс «Обеспечение непрерывности ведения бизнеса».	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Выполнение лабораторной работы, подготовка к устному ответу.
8.	Обеспечение соответствия требованиям законодательства РФ.	Конспектирование материала на лекционных занятиях. Подготовка к докладу. Работа с учебной литературой. Выполнение лабораторной работы, подготовка к устному ответу.

Порядок выполнения каждого вида самостоятельной работы:

1. Конспектирование и проработка лекционного материала.
2. Работа с основной и дополнительной литературой.
3. Анализ и проработка результатов лабораторного занятия.
4. Подготовка доклада.

Контроль за самостоятельной работой осуществляется во время лекционных и лабораторных занятий, а также во время финального испытания (зачет).

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения зачета – зачёт.

Вопросы к зачёту:

1. Процессный подход к построению СУИБ и циклическая модель PDCA.
2. Цели и задачи, решаемые СУИБ.
3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Стратегии выбора области деятельности СУИБ.

5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
6. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
7. Политика ИБ и политика СУИБ: сходства и различия.
8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
16. Внедрение процессов управления ИБ: этапы и последовательность.
17. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания

1.	ПК-12 - способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;	Знает: историю информационных технологий; основные направления повышения надежности вычислительных систем, комплексов и сетей, а также методы и средства обеспечения безопасности и сохранности информации в них; Умеет: понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны; анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ.	Лабораторные работы, собеседования, доклад, вопросы к зачету	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п.4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-18 - способность	Знает: основные принципы	Лабораторные работы,	
	организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	построения информационной безопасности; Умеет: использовать современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;	собеседования, доклад, вопросы к зачету	

3.	ПК-19 - способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Знает: основные стандарты, регламентирующие управление ИБ; способы защиты информации в различных операционных системах; Умеет: практически решать задачи формализации разрабатываемых процессов управления ИБ; выделять основные методы организации информационной безопасности в условиях конкретной задачи;	Лабораторные работы, собеседования, доклад, вопросы к зачету	
4.	ПК-28 - способность управлять информационной безопасностью автоматизированной системы	Знает: основные стандарты, регламентирующие управление ИБ; принципы разработки процессов управления ИБ; Умеет: определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ.	Лабораторные работы, собеседования, доклад, вопросы к зачету	

* - не предусмотрен

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. **Клименко, И.С.** Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2020. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-516-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1018665 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

7.2. Дополнительная литература:

1. **Гришина, Н. В.** Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - Москва :Форум, НИЦ ИНФРА-М, 2016. - 240 с. (Высшее образование: Бакалавриат) (Обложка. КБС)ISBN 978-5-00091-007-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/544554 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

2. **Варфоломеева, А. О.** Информационные системы предприятия: Учебное пособие / Варфоломеева А. О., Коряковский А. В., Романов В. П. - Москва : НИЦ ИНФРА-М, 2016. -

283 с. (Высшее образование: Бакалавриат) ISBN 978-5-16-005549-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/536732 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

7.3. Интернет-ресурсы

- Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [On-line] (дата обращения: 15.05.2020).

7.4 Современные профессиональные базы данных и информационные справочные системы:

- Национальная электронная библиотека. - https://rusneb.ru/ [On-line] (дата обращения: 15.05.2020).

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Лицензионное ПО:**
  платформа для электронного обучения Microsoft Teams; MS Visual Studio; MS SQL Server.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

- лекционная аудитория с проектором;
- компьютерный класс.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
“01” июня 2020 г.

СОВРЕМЕННЫЕ СИСТЕМЫ ВИРТУАЛИЗАЦИИ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность распределенных компьютерных систем»
форма обучения очная

Оленников Е.А., Оленников А.А. Современные системы виртуализации. Рабочая программа для обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Современные системы виртуализации [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Оленников Е.А., Оленников А.А. 2020.

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ОК-8, ПК-17.

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

В результате освоения дисциплины обучающиеся будут
Знать:

- технологии для DevOps;
- технологии виртуализации;
- гипервизоры 1,2 уровней;
- методы обеспечения отказоустойчивости;
- методы резервного копирования;
- принципы функционирования Docker;
- kubernetes и оркестрацию контейнеров;
- технологию централизованного управления логами;
- компоненты ИТ-инфрасруктуры;
- особенности операционных систем (ОС) Linux;
- основные принципы и команды CLI;
- основы администрирования в ОС Linux;

Уметь:

- устанавливать и настраивать основные инфраструктурные компоненты для проектирования и разработки информационных систем;
- выполнять базовые функции администрирования ОС Linux;
- работать с CLI и системными утилитами;
- конфигурировать локальные сети;
- устанавливать и настраивать инструменты разработчика и необходимые библиотеки;
- управлять репозиторием проекта (локальным и удалённым);
- настраивать гипервизоры 1,2 уровней;
- настраивать и проводить мониторинг инфраструктуры;
- настраивать централизованное управление логами;
- работать с Graylog, ELK, RabbitMQ, Zabbix.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			10
Общая трудоемкость	**зач. ед.**	5	5
	час	180	180
Из них:			
Часы аудиторной работы (всего):		64	64
Лекции		32	32
Практические занятия		32	32
Лабораторные / практические занятия по подгруппам		0	0

Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося	116	116
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)		Зачет

3. Система оценивания.

Обучающиеся, не набравшие 61 балла в течение семестра, или не согласные с оценкой, полученной по итогам текущего контроля в семестре, проходят промежуточную аттестацию в форме зачета – 10 семестр.

При проведении промежуточной аттестации результаты, полученные обучающимся в семестре, переводятся в формат традиционной оценки в соответствии со шкалой перевода баллов:

– от 0 до 60 баллов – «не зачтено»;
– от 61 до 100 баллов – «зачтено».

– 60 баллов и менее – «неудовлетворительно»;
– от 61 до 75 баллов – «удовлетворительно»;
– от 76 до 90 баллов – «хорошо»;
– от 91 до 100 баллов – «отлично».

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№	Тематика учебных встреч	Виды аудиторной работы (в ак.час.)			Итого аудиторных ак.часов по теме
		Лекции	Практические занятия	Лабораторные / практические занятия по подгруппам	
1	2	3	4	5	6
	Часов в 6 семестре	32	0	32	64
	Современные системы виртуализации	32	0	32	64
1	Лекция 1	2	0	0	2
2	Лабораторная работа 1	0	0	2	2
3	Лекция 2	2	0	0	2
4	Лабораторная работа 2	0	0	2	2
5	Лекция 3	2	0	0	2
6	Лабораторная работа 3	0	0	2	2
7	Лекция 4	2	0	0	2
8	Лабораторная работа 4	0	0	2	2
9	Лекция 5	2	0	0	2
10	Лабораторная работа 5	0	0	2	2
11	Лекция 6	2	0	0	2
12	Лабораторная работа 6	0	0	2	2
13	Лекция 7	2	0	0	2
14	Лабораторная работа 7	0	0	2	2
15	Лекция 8	2	0	0	2
16	Лабораторная работа 8	0	0	2	2
17	Лекция 9	2	0	0	2

18	Лабораторная работа 9	0	0	2	2
19	Лекция 10	2	0	0	2
20	Лабораторная работа 10	0	0	2	2
21	Лекция 11	2	0	0	2
22	Лабораторная работа 11	0	0	2	2
23	Лекция 12	2	0	0	2
24	Лабораторная работа 12	0	0	2	2
25	Лекция 13	2	0	0	2
26	Лабораторная работа 13	0	0	2	2
27	Лекция 14	2	0	0	2
28	Лабораторная работа 14	0	0	2	2
29	Лекция 15	2	0	0	2
30	Лабораторная работа 15	0	0	2	2
31	Лекция 16	2	0	0	2
32	Лабораторная работа 16	0	0	2	2
33	Консультация по ССВирт	0	0	0	0
34	Консультация по ССВирт	0	0	0	0
35	Экзамен ССВирт	0	0	0	0
	Итого (ак.часов)	32	0	32	64

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Лекция 1	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
2.	Лекция 2	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
3.	Лекция 3	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
4.	Лекция 4	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
5.	Лекция 5	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
6.	Лекция 6	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
7.	Лекция 7	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
8.	Лекция 8	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
9.	Лекция 9	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
10.	Лекция 10	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
11.	Лекция 11	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
12.	Лекция 12	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.

13.	Лекция 13	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
14.	Лекция 14	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
15.	Лекция 15	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.
16.	Лекция 16	Чтение обязательной и дополнительной литературы, подготовка к практическим работам.

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение рекомендованной основной и дополнительной литературы.
3. Выполнение практических работ.

Контроль за самостоятельной работой осуществляется при выполнении обучающимся практической работы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Форма проведения промежуточной аттестации – зачет. Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса.

Вопросы к зачету.

1. Методология DevOps и ее основные цели.
2. Гибкая методология разработки.
3. Гибкие методики разработки.
4. Методология Agile. Примеры метолодолий.
5. Основные идеи и основополагающие принципы Agile Manifesto.
6. Непрерывное тестирование и Непрерывный мониторинг.
7. Микросервисы,Инфраструктура как код.
8. Технологии для DevOps Bash и -Docker.
9. Оркестрация. Kubernetes. CI/CD-системы.
10. Облачные серверы. Системы конфигурации.
11. Системы мониторинга. Языки программирования. Базы данных.
12. Виртуализация, эмуляция, симуляция.
13. Гипервизор первого типа (bare-metal) и второго типа (hosted).
14. Технологии виртуализации. Гипервизоры 1,2 уровня.
15. Системы хранения данных и способ выделения ресурсов.
16. Облачные сервисы AWS, GoogleCloud, Базис основные особенности и отличия.
17. Полная виртуализация и неполная виртуализация. Отличия, достоинства и недостатки.
18. Масштабируемость и отказоустойчивость. Методы обеспечения отказоустойчивости.
19. Кластеризация (Pacemaker).
20. Способы и методы резервного копирования. Особенности настройки.
21. Балансировка нагрузки. HAProxy/Nginx Disaster recovery. Keepalived/vrrp.
22. Способы организации отказоустойчивости в облаке.
23. Управление инфраструктурой.Terraform. Управление конфигурацией Ansible.
24. Системы контроля версий. Распределённая система управления версиями Git.
25. Docker. Основные понятия, назначение и применение.
26. Микросервисная архитектура. Основное назначение, история развития.

27. Непрерывная интеграция (CI) и непрерывная поставка (CD).
28. Интрументы Jenkins, TeamCity, Gitlab. Особенности, отличия, применение.
29. Мониторинг инфраструктуры. Централизованное управление логами.
30. Инструмент Graylog и его возможности.
31. Система визуализации, мониторинга и анализа данных Grafana и ELK.
32. Менеджер очередей RabbitMQ.
33. Сбор и анализ ошибок при помощи Sentry.
34. Инцидент-менеджмент Zabbix. Особенности, основное назначение, способы настройки на примере.

Возможные альтернативные задания для проверочной итоговой аттестации:

1. Развёртывание PostgreSQL версии не ниже 12. Создание базы данных из четырех столбцов произвольного названия. Наполнить произвольными тестовыми данными, не менее 10-ти значений (Модуль: Администрирование баз данных).
2. На основе созданной БД из Модуля 6 создаем кластер из двух nod в реплике конфигурации Active/Passive
3. Установка и развертывание Prometheus+Grafana+Node_exporter. Настройка метрик нагрузки вашей ОС с отображением в Grafana
4. Развертывание ВМ в Базисе на базе шаблона Ubuntu 20.04 LTS. Установка на нее пакетов: vim, mc, net-tools
5. Развёртывание ВМ в БАЗИС на базе шаблона Ubuntu 20.04 LTS с использованием Terraform* + provider для БАЗИСА
6. Создание 2 ВМ на базе шаблона CentOS 7.9, установка на них ansible и настройка. Создание ansible-playbook по созданию 2 папок, 1 пользователя, установки пакетов vim, mc с 1 ВМ на 2 ВМ
7. Установка git на ВМ, создать репозиторий в предварительно подготовленном сервере Git с пустым файлом Readme.md, клонировать репозитория на локаль, сделать commit с Readme.md в новой ветке с последующим merge branch в удаленном репозиторий в master.
8. Создание ВМ, установка на нём Jenkins, развёртывание с помощью Jenkins https://github.com/AliyunContainerService/redis-cluster на ВМ
9. Создание dockerfile на базе образа centos 7.9, в него установить PostgreSQL версии не ниже 12, добавить пользователя в БД, создать в БД 2 таблицы и наполнить их на 10 значений. Скрипты и наполнение можно взять из модуля 6. Собрать полученый docker image через docker build и запустить. Подключиться с хостовой машины к инсталлированному PostgreSQL утилитой psql.
10. Создать свой docker-compose file на базе v3, в котором описать развёртывание в одном контейнере PHP+ tomcat 8 и во втором пустой БД MariaDB, в которой будет замаплен локальный volume ./ mysql /. Собрать и запустить, показать страницу php из браузера и доступность порта MariaDB
11. Развернуть k8s v 1.26 кластер, состоящий из 1 master и 1 worker node и установить на worker node RabbitMQ через Helm-chart
12. Написать Helm-chart по управлению k8s cluster из п.17. Установить в k8s cluster из п.17, Prometheus+Grafana
13. В k8s cluser из п.17 создать namespace vault и установить с помощью helm-chart hashicorp vault последней версии, настроить под него persistent volume с 10 GB. Создать ns app_test с лимитом 20mlcore, 2GB memory и установить туда haproxy с авторизацией в stats, ключ авторизации должен храниться в vault и быть вынесен в ENV pod сервиса.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ОК-8 - способность к самоорганизации и самообразованию	**Знать:** технологии для DevOps; технологии виртуализации; гипервизоры 1,2 уровней; методы обеспечения отказоустойчивости; методы резервного копирования; принципы функционирования Docker. **Уметь:** устанавливать и настраивать основные инфраструктурные компоненты для проектирования и разработки информационных систем; выполнять базовые функции администрирования ОС Linux; работать с CLI и системными утилитами; конфигурировать локальные сети; устанавливать и настраивать инструменты разработчика и необходимые библиотеки.	Собеседование, практические работы, билеты к зачету.	Компетенции сформированы при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-17 - способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления	**Знать:** kubernetes и оркестрацию контейнеров; технологию централизованного управления логами; компоненты ИТ-инфраструктуры; особенности операционных систем (ОС) Linux; основные принципы и команды CLI; основы администрирования в ОС Linux. **Уметь:** управлять репозиторием проекта (локальным и удалённым); настраивать гипервизоры 1,2 уровней;	Собеседование, практические работы, билеты к зачету.	Компетенции сформированы при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена

	базами данных, сетевое программное обеспечение.	настраивать и проводить мониторинг инфраструктуры; настраивать централизованное управление логами; работать с Graylog, ELK, RabbitMQ, Zabbix.		согласно требованиям п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Форсгрен, Н. Ускоряйся! Наука DevOps: как создавать и масштабировать высокопроизводительные цифровые организации / Николь Форсгрен, Джез Хамбл, Джин Ким ;пер. с англ. А. Техненко. - Москва : Интеллектуальная Литература, 2020. - 216 с. - ISBN 978-5-6042881-1-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1222488 (дата обращения: 27.07.2023). – Режим доступа: по подписке.
2. Гунько, А. В. Системное программирование в среде Linux : учебное пособие / А. В. Гунько. - Новосибирск : Изд-во НГТУ, 2020. - 235 с. - ISBN 978-5-7782-4160-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1870577 (дата обращения: 27.07.2023). – Режим доступа: по подписке.

7.2. Дополнительная литература:

1. Губарев, В. В. Введение в облачные вычисления и технологии / Губарев В.В., Савульчик С.А. - Новосибирск :НГТУ, 2013. - 48 с.: ISBN 978-5-7782-2252-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/557005 (дата обращения: 27.07.2023). – Режим доступа: по подписке.
2. Максимов, Н. В. Компьютерные сети : учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2023. — 464 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-454-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1921406 (дата обращения: 27.07.2023). – Режим доступа: по подписке.

7.3. Интернет-ресурсы

1. Научная электронная библиотека. URL: http://elibrary.ru/.
2. Электронные ресурсы ИБЦ ТюмГУ. URL: https://bmk.utmn.ru/ru/.

7.4 Современные профессиональные базы данных и информационные справочные системы

- Межвузовская электронная библиотека (МЭБ). - URL: https://icdlib.nspu.ru/
- Национальная электронная библиотека. - URL: https://rusneb.ru/
- Institute of Electrical and Electronics Engineers, Inc (IEEE). - URL: https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
- Orbit Intelligence. - URL: https://www.orbit.com

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Лицензионное ПО:

- Microsoft Imagine Academy (ранее Dreamspark): ОС семейства MS Windows (редакция Pro/Server);
- Офисный пакет Microsoft Office 365 (лицензионное соглашение №2т/00509-20 от 12.05.2020);
- Платформа для электронного обучения Microsoft Teams.

- Свободно распространяемое ПО:
  - Программное обеспечение виртуализации: VirtualBox (бесплатная лицензия доступна: https://www.virtualbox.org/wiki/Downloads).

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения лекций и практических занятий;

Лаборатории, оснащенные лабораторным оборудованием в соответствии с ФГОС ВО 3+ по данному направлению.