ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместителем директора
института Переваловой М.Н.
РАЗРАБОТЧИК(И)
Оленников Е. А.

Администрирование операционных систем

Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01. Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ОПК-12.

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Зания:

- основные задачи и функции администратора ОС;
- знать типы, версии и редакции ОС Windows, Linux, Unix;
- основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности;
- знать основные команды, применяемые при администрировании ОС Windows, Linux, Unix;
- основы разработки сценариев;
- базовые задачи по обеспечению защиты ОС, вычислительных ресурсов ЭВМ и данных;
- основные электронные ресурсы по теме безопасного администрирования ОС.

Умения:

- 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;
- 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.

Навыки:

- базового администрирования ОС Windows, Linux, Unix;
- работы в командной строке;
- написания и выполнение административных сценариев;
- навыками поиска технической информации.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**	
			5	6
Общая трудоемкость	**зач. ед.**	8	4	4
	час	288	144	144
Из них:				
Часы аудиторной работы (всего):		128	64	64
Лекции		64	32	32
Практические занятия		0	0	0

Лабораторные / практические занятия по подгруппам	64	32	32
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося	160	80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)		Дифференцированный зачет	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 5 семестре	32	0	32	64
	Администрирование операционных систем 1	32	0	32	64
1	Лекционное занятие 1.	2	0	0	2
2	Лабораторное занятие 1	0	0	2	2
3	Лекционное занятие 2.	2	0	0	2
4	Лабораторное занятие 2	0	0	2	2
5	Лекционное занятие 3.	2	0	0	2
6	Лабораторное занятие 3	0	0	2	2
7	Лекционное занятие 4.	2	0	0	2
8	Лабораторное занятие 4	0	0	2	2
9	Лекционное занятие 5.	2	0	0	2
10	Лабораторное занятие 5	0	0	2	2
11	Лекционное занятие 6.	2	0	0	2
12	Лабораторное занятие 6	0	0	2	2
13	Лекционное занятие 7.	2	0	0	2
14	Лабораторное занятие 7	0	0	2	2
15	Лекционное занятие 8.	2	0	0	2
16	Лабораторное занятие 8	0	0	2	2
17	Лекционное занятие 9.	2	0	0	2
18	Лабораторное занятие 9	0	0	2	2
19	Лекционное занятие 10.	2	0	0	2
20	Лабораторное занятие 10	0	0	2	2
21	Лекционное занятие 11.	2	0	0	2
22	Лабораторное занятие 11	0	0	2	2
23	Лекционное занятие 12.	2	0	0	2
24	Лабораторное занятие 12	0	0	2	2
25	Лекционное занятие 13.	2	0	0	2
26	Лабораторное занятие 13	0	0	2	2
27	Лекционное занятие 14.	2	0	0	2
28	Лабораторное занятие 14	0	0	2	2
29	Лекционное занятие 15.	2	0	0	2
30	Лабораторное занятие 15	0	0	2	2
31	Лекционное занятие 16.	2	0	0	2

32	Лабораторное занятие 16	0	0	2	2
33	Консультация перед зачетом	0	0	0	0
34	Зачет по дисциплине	0	0	0	0
	Часов в 6 семестре	32	0	32	64
	Администрирование операционных систем 2	32	0	32	64
1	Лекционное занятие 1.	2	0	0	2
2	Лабораторное занятие 1	0	0	2	2
3	Лекционное занятие 2.	2	0	0	2
4	Лабораторное занятие 2	0	0	2	2
5	Лекционное занятие 3.	2	0	0	2
6	Лабораторное занятие 3	0	0	2	2
7	Лекционное занятие 4.	2	0	0	2
8	Лабораторное занятие 4	0	0	2	2
9	Лекционное занятие 5.	2	0	0	2
10	Лабораторное занятие 5	0	0	2	2
11	Лекционное занятие 6.	2	0	0	2
12	Лабораторное занятие 6	0	0	2	2
13	Лекционное занятие 7.	2	0	0	2
14	Лабораторное занятие 7	0	0	2	2
15	Лекционное занятие 8.	2	0	0	2
16	Лабораторное занятие 8	0	0	2	2
17	Лекционное занятие 9.	2	0	0	2
18	Лабораторное занятие 9	0	0	2	2
19	Лекционное занятие 10.	2	0	0	2
20	Лабораторное занятие 10	0	0	2	2
21	Лекционное занятие 11.	2	0	0	2
22	Лабораторное занятие 11	0	0	2	2
23	Лекционное занятие 12.	2	0	0	2
24	Лабораторное занятие 12	0	0	2	2
25	Лекционное занятие 13.	2	0	0	2
26	Лабораторное занятие 13	0	0	2	2
27	Лекционное занятие 14.	2	0	0	2
28	Лабораторное занятие 14	0	0	2	2
29	Лекционное занятие 15.	2	0	0	2
30	Лабораторное занятие 15	0	0	2	2
31	Лекционное занятие 16.	2	0	0	2
32	Лабораторное занятие 16	0	0	2	2
33	Консультация перед экзаменом	0	0	0	0
34	Экзамен по дисциплине	0	0	0	0
	Итого (ак.часов)	64	0	64	128

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 диф. зачета – 5 семестр, экзамена – 6 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 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: 15.05.2022).

2. 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: 15.05.2022).

3. 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: 15.05.2022).

5.2 Электронные образовательные 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/

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека https://rusneb.ru/

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

MS Office, платформа для электронного обучения Microsoft Teams, ОС MS Windows, ОС FreeBSD.

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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
И.П. Петров, Т.И. Паюсова

АНАЛИЗ И УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01. Компьютерная безопасность
специализация Безопасность компьютерных систем и сетей
(связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-4.2*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Анализ и управление рисками информационной безопасности

Знать:

1) Основные определения и термины из области анализа и оценки рисков информационной безопасности;

2) Методики анализа и оценки рисков информационной безопасности;

3) Принципы построения и сопровождения системы управления информационными рисками и системы управления информационной безопасностью.

Уметь:

1) Определять субъекты и объекты информационной системы;

2) Составлять модель угроз и модель злоумышленника;

3) Разрабатывать политику информационной безопасности;

4) Анализировать и оценивать риски информационной безопасности;

5) Внедрять и сопровождать систему управления информационными рисками и систему управления информационной безопасностью.

Владеть:

1) Навыками разработки документации стратегического и тактического уровней;

2) Инструментами реализации системы управления информационными рисками и системы управления информационной безопасностью;

3) Навыками расчёта величины риска информационной безопасности.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			9
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося		80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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 9 семестре	32	0	32	64
	Анализ и управление рисками информационной безопасности	32	0	32	64
1	Аудит информационной безопасности	2	0	0	2
2	Сущности информационной безопасности	0	0	2	2
3	Определение риска информационной безопасности	2	0	0	2
4	Анализ рисков информационной безопасности	0	0	2	2
5	Работа с учебной литературой, конспектом лекции и выполнение домашнего практического задания	0	0	0	0
6	Анализ и оценка рисков информационной безопасности	2	0	0	2
7	Анализ текущего уровня защищенности информационной системы	0	0	2	2
8	Управление рисками информационной безопасности	2	0	0	2
9	Система защиты информации	0	0	2	2
10	Работа с учебной литературой, конспектом лекции и выполнение домашнего практического задания	0	0	0	0
11	Цикл Деминга-Шухарта	2	0	0	2
12	Принцип глубокой эшелонированности обороны	0	0	2	2
13	Обзор серий стандартов ISO 27000	2	0	0	2
14	Система управления информационными рисками	0	0	2	2
15	Работа с учебной литературой, конспектом лекции и выполнение домашнего практического задания	0	0	0	0
16	Система управления информационными рисками (СУИР)	2	0	0	2

17	Типовые документы по информационной безопасности	0	0	2	2
18	Нормативная и операционная документация при построении СУИР	2	0	0	2
19	Документы стратегического и тактического уровней в информационной безопасности	0	0	2	2
20	Работа с учебной литературой, конспектом лекции и выполнение домашнего практического задания	0	0	0	0
21	Ожидаемые среднегодовые потери	2	0	0	2
22	Ожидаемые среднегодовые потери	0	0	2	2
23	Возврат инвестиций в информационную безопасность	2	0	0	2
24	Возврат инвестиций в информационную безопасность	0	0	2	2
25	Работа с учебной литературой, конспектом лекции и выполнение домашнего практического задания	0	0	0	0
26	Политика безопасности	2	0	0	2
27	Разграничение прав доступа в системе	0	0	2	2
28	Модели свойств безопасности	2	0	0	2
29	Обеспечение свойств информации с точки зрения информационной безопасности	0	0	2	2
30	Работа с учебной литературой, конспектом лекции и выполнение домашнего практического задания	0	0	0	0
31	Библиотека инфраструктуры информационных технологий (ITIL)	2	0	0	2
32	Инциденты информационной безопасности	0	0	2	2
33	Управление инцидентами информационной безопасности	2	0	0	2
34	Управление инцидентами информационной безопасности	0	0	2	2
35	Работа с учебной литературой, конспектом лекции и выполнение домашнего практического задания	0	0	0	0
36	Статистическая обработка данных в задачах информационной безопасности	2	0	0	2
37	Анализ данных в задачах информационной безопасности	0	0	2	2
38	Работа с учебной литературой, конспектом лекции и выполнение домашнего практического задания	0	0	0	0
39	Интеллектуальный анализ данных в информационной безопасности	2	0	0	2
40	Интеллектуальный анализ данных в информационной безопасности	0	0	2	2

41	Консультация	0	0	0	0
42	Консультация	0	0	0	0
43	Работа с учебной литературой, конспектом лекции и выполнение домашнего практического задания	0	0	0	0
44	Дифференцированный зачет	0	0	0	0
	Итого (ак.часов)	32	0	32	64

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 дифференцированный зачет (6 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вешах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

2. Белоус, А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения : практическое пособие / А. И. Белоус. - Москва ; Вологда : Инфра-Инженерия, 2020. - 644 с. - ISBN 978-5-9729-0512-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167734 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

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: 31.08.2022). – Режим доступа: по подписке.

4. Клименко, И.С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651 (дата обращения: дата обращения: 31.08.2022). – Режим доступа: по подписке.

5. Мосолов, А.С. Компьютерные технологии и методы проектирования в сфере безопасности : учебник для вузов / А. С. Мосолов, Н. И. Акинин. — Санкт-Петербург : Лань, 2021. — 444 с. — ISBN 978-5-8114-8034-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183115 (дата обращения: 31.08.2022). — Режим доступа: для авториз. пользователей.

6. Сычев, Ю.Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование:

Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:

- Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [On-line] (дата обращения: 31.08.2022).

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека. URL: https://rusneb.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.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
заместитель директора
Института математики и
компьютерных наук
Перевалова М. Н.
РАЗРАБОТЧИК(И)
Ханбеков Ш. И.

Большие данные

Рабочая программа
для обучающихся по специальности 10.05.01 Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
Уровень высшего образования: специалитет
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ОПК-8

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Большие данные

В результате освоения дисциплины студент должен:
знать:

- принципы и методы хранения и обработки данных большого объема;
- основы администрирования систем хранения и обработки больших данных;
- теоретические основы анализа данных;
- технологии, используемые в современных системах хранения и обработки больших данных;
- особенности защиты информации в системах хранения и обработки больших данных;

уметь:

- обосновать выбор стека технологий для хранения и обработки данных большого объема;
- администрировать системы хранения и обработки больших данных;
- использовать технологии для анализа данных большого объема;
- оптимизировать выполнение задач над данными большого объема;
- применять инструментарий обеспечения информационной безопасности в системах хранения и обработки больших данных.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			9
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося		80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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 9 семестре	32	32	0	64
	Большие данные	32	32	0	64
1	Вводная лекция	2	0	0	2
2	Основы применения технологий Big Data	0	2	0	2
3	NoSQL	2	0	0	2
4	Практическое применение NoSQL	0	2	0	2
5	Фреймворк Apache Hadoop. Основы	4	0	0	4
6	Установка и базовая конфигурация Apache Hadoop	0	2	0	2
7	Работа с HDFS. Запуск задач MapReduce	0	2	0	2
8	Введение в анализ данных	4	0	0	4
9	Типовые задачи Apache Hadoop	0	2	0	2
10	Алгоритмы на графах в MapReduce	0	2	0	2
11	Информационная безопасность Apache Hadoop	4	0	0	4
12	Конфигурация Apache Hadoop в защищенном исполнении	0	2	0	2
13	Apache Knox. Apache Atlas. Apache Ranger	0	2	0	2
14	Фреймворк Apache Hadoop. Продвинутый уровень	4	0	0	4
15	Java API. Начало	0	2	0	2
16	Java API. Продолжение	0	2	0	2
17	Фреймворк Apache Hadoop. Системы управления базами данных	4	0	0	4
18	Apache Pig	0	2	0	2
19	Apache Hive	0	2	0	2
20	Фреймворк Apache Hadoop. Альтернативные инструменты анализа данных	4	0	0	4
21	Apache HBase	0	2	0	2
22	Apache Cassandra	0	2	0	2

23	Фреймворк Apache Spark	4	0	0	4
24	Установка и конфигурация Apache Spark	0	2	0	2
25	Практическое применение Apache Spark	0	2	0	2
26	Консультация	0	0	0	0
27	Дифференцированный зачет	0	0	0	0
	Итого (ак.часов)	32	32	0	64

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 собеседования по билетам. Собеседование включает один теоретический вопрос и одно практическое задание.

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. 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 с. — ISBN 978-5-4497-0289-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89404.html (дата обращения: 12.05.2022). — Режим доступа: для авторизир. пользователей.

2. Дадян, Э. Г. Данные: хранение и обработка : учебник / Э. Г. Дадян. — Москва : ИНФРА-М, 2021. — 205 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-016447-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1149101 (дата обращения: 12.05.2022). – Режим доступа: по подписке.

3. Щербакова, Ю. В. Теория вероятностей и математическая статистика: учебное пособие / Ю. В. Щербакова. — 2-е изд. — Саратов : Научная книга, 2019. — 159 с. — ISBN 978-5-9758-1786-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/81056.html (дата обращения 12.05.2022). – Режим доступа для авторизир. пользователей.

5.2 Электронные образовательные ресурсы:

- вузовские электронно-библиотечные системы учебной литературы;
- вузовские электронно-библиотечные системы учебной литературы;
- база научно-технической информации ВИНИТИ РАН;
- доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, mathnet.ru;

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека. URL: https://rusneb.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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
М.Б. Атманских

Дополнительные главы математики
Рабочая программа
Специальность: 10.05.01. Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-3*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Дополнительные главы математики

Знать

- совокупности математических методов

Уметь

- разрабатывать, обосновывать и реализовывать процедуры решения задач

профессиональной деятельности;

- способен использовать математические методы, необходимые для решения задач профессиональной деятельности;

Владеть

- необходимыми математическими методами для решения задач профессиональной деятельности.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			5
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося		80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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 5 семестре	32	32	0	64
	Дополнительные главы математики	32	32	0	64
1	Лекционное занятие 1	2	0	0	2
2	Практическое занятие 1	0	2	0	2
3	Лекционное занятие 2	2	0	0	2
4	Практическое занятие 2	0	2	0	2
5	Лекционное занятие 3	2	0	0	2
6	Практическое занятие 3	0	2	0	2
7	Лекционное занятие 4	2	0	0	2
8	Практическое занятие 4	0	2	0	2
9	Лекционное занятие 5	2	0	0	2
10	Практическое занятие 5	0	2	0	2
11	Лекционное занятие 6	2	0	0	2
12	Практическое занятие 6	0	2	0	2
13	Лекционное занятие 7	2	0	0	2
14	Практическое занятие 7	0	2	0	2
15	Лекционное занятие 8	2	0	0	2
16	Практическое занятие 8	0	2	0	2
17	Лекционное занятие 9	2	0	0	2
18	Практическое занятие 9	0	2	0	2
19	Лекционное занятие 10	2	0	0	2
20	Практическое занятие 10	0	2	0	2
21	Лекционное занятие 11	2	0	0	2
22	Практическое занятие 11	0	2	0	2
23	Лекционное занятие 12	2	0	0	2
24	Практическое занятие 12	0	2	0	2
25	Лекционное занятие 13	2	0	0	2
26	Практическое занятие 13	0	2	0	2
27	Лекционное занятие 14	2	0	0	2
28	Практическое занятие 14	0	2	0	2

29	Лекционное занятие 15	2	0	0	2
30	Практическое занятие 15	0	2	0	2
31	Лекционное занятие 16	2	0	0	2
32	Практическое занятие 16	0	2	0	2

33	Консультация	0	0	0	0
34	Аттестация 1	0	0	0	0
	Итого (ак.часов)	32	32	0	64

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 дифференцированный зачет (5 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

2. Белоус, А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения : практическое пособие / А. И. Белоус. - Москва ; Вологда : Инфра-Инженерия, 2020. - 644 с. - ISBN 978-5-9729-0512-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167734 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

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: 31.08.2022). – Режим доступа: по подписке.

4. Клименко, И.С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651 (дата обращения: дата обращения: 31.08.2022). – Режим доступа: по подписке.

5. Мосолов, А.С. Компьютерные технологии и методы проектирования в сфере безопасности : учебник для вузов / А. С. Мосолов, Н. И. Акинин. — Санкт-Петербург : Лань, 2021. — 444 с. — ISBN 978-5-8114-8034-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183115 (дата обращения: 31.08.2022). — Режим доступа: для авториз. пользователей.

6. Сычев, Ю.Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование:

Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:

- Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [Online] (дата обращения: 31.08.2022).

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека. URL: https://rusneb.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.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
М.Б. Атманских

Дополнительные главы математической статистики

Рабочая программа
Специальность: 10.05.01. Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-3*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Дополнительные главы математической статистики

Знать

- совокупности математических методов

Уметь

- разрабатывать, обосновывать и реализовывать процедуры решения задач

профессиональной деятельности;

- способен использовать математические методы, необходимые для решения задач профессиональной деятельности;

Владеть

- необходимыми математическими методами для решения задач профессиональной деятельности.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			6
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося		80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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 6 семестре	32	32	0	64
	Дополнительные главы математической статистики	32	32	0	64
1	Лекционное занятие 1	2	0	0	2
2	Практическое занятие 1	0	2	0	2
3	Лекционное занятие 2	2	0	0	2
4	Практическое занятие 2	0	2	0	2
5	Лекционное занятие 3	2	0	0	2
6	Практическое занятие 3	0	2	0	2
7	Лекционное занятие 4	2	0	0	2
8	Практическое занятие 4	0	2	0	2
9	Лекционное занятие 5	2	0	0	2
10	Практическое занятие 5	0	2	0	2
11	Лекционное занятие 6	2	0	0	2
12	Практическое занятие 6	0	2	0	2
13	Лекционное занятие 7	2	0	0	2
14	Практическое занятие 7	0	2	0	2
15	Лекционное занятие 8	2	0	0	2
16	Практическое занятие 8	0	2	0	2
17	Лекционное занятие 9	2	0	0	2
18	Практическое занятие 9	0	2	0	2
19	Лекционное занятие 10	2	0	0	2
20	Практическое занятие 10	0	2	0	2
21	Лекционное занятие 11	2	0	0	2
22	Практическое занятие 11	0	2	0	2
23	Лекционное занятие 12	2	0	0	2
24	Практическое занятие 12	0	2	0	2
25	Лекционное занятие 13	2	0	0	2
26	Практическое занятие 13	0	2	0	2

27	Лекционное занятие 14	2	0	0	2
28	Практическое занятие 14	0	2	0	2
29	Лекционное занятие 15	2	0	0	2
30	Практическое занятие 15	0	2	0	2
31	Лекционное занятие 16	2	0	0	2
32	Практическое занятие 16	0	2	0	2
33	Консультация	0	0	0	0
34	Аттестация 1	0	0	0	0
	Итого (ак.часов)	32	32	0	64

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 дифференцированный зачет (6 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вешах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

2. Белоус, А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения : практическое пособие / А. И. Белоус. - Москва ; Вологда : Инфра-Инженерия, 2020. - 644 с. - ISBN 978-5-9729-0512-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167734 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

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: 31.08.2022). – Режим доступа: по подписке.

4. Клименко, И.С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651 (дата обращения: дата обращения: 31.08.2022). – Режим доступа: по подписке.

5. Мосолов, А.С. Компьютерные технологии и методы проектирования в сфере безопасности : учебник для вузов / А. С. Мосолов, Н. И. Акинин. — Санкт-Петербург : Лань, 2021. — 444 с. — ISBN 978-5-8114-8034-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183115 (дата обращения: 31.08.2022). — Режим доступа: для авториз. пользователей.

6. Сычев, Ю.Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:

- Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [Online] (дата обращения: 31.08.2022).

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека. URL: https://rusneb.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.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместителем директора
института Переваловой М.Н.
РАЗРАБОТЧИК(И)
Оленников Е. А.

Защита в операционных системах

Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01. Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ОПК-12.

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Знания:

- 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;
- содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности;

Умения:

- 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;
- конфигурировать встроенные сервисы безопасности ОС;
- проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
- проводить инструментальный контроль защищенности ОС;
- самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;

Навыки:

- поиска и анализа информации об уязвимостях ОС;
- анализ угроз информационной безопасности в ОС;
- безопасного администрирования ОС;
- оценки уровня безопасности ОС;
- использования средств инструментального контроля защищенности ОС.

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.**	8	4	4
	час	288	144	144
Из них:				
Часы аудиторной работы (всего):		124	64	60
Лекции		62	32	30
Практические занятия		0	0	0

Лабораторные / практические занятия по подгруппам	62	32	30
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося	164	80	84
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)		Дифференцированный зачет	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 7 семестре	32	0	32	64
	Защита в операционных системах 1	32	0	32	64
1	Лекционное занятие 1.	2	0	0	2
2	Лабораторное занятие 1	0	0	2	2
3	Лекционное занятие 2.	2	0	0	2
4	Лабораторное занятие 2	0	0	2	2
5	Лекционное занятие 3.	2	0	0	2
6	Лабораторное занятие 3	0	0	2	2
7	Лекционное занятие 4.	2	0	0	2
8	Лабораторное занятие 4	0	0	2	2
9	Лекционное занятие 5.	2	0	0	2
10	Лабораторное занятие 5	0	0	2	2
11	Лекционное занятие 6.	2	0	0	2
12	Лабораторное занятие 6	0	0	2	2
13	Лекционное занятие 7.	2	0	0	2
14	Лабораторное занятие 7	0	0	2	2
15	Лекционное занятие 8.	2	0	0	2
16	Лабораторное занятие 8	0	0	2	2
17	Лекционное занятие 9.	2	0	0	2
18	Лабораторное занятие 9	0	0	2	2
19	Лекционное занятие 10.	2	0	0	2
20	Лабораторное занятие 10	0	0	2	2
21	Лекционное занятие 11.	2	0	0	2
22	Лабораторное занятие 11	0	0	2	2
23	Лекционное занятие 12.	2	0	0	2
24	Лабораторное занятие 12	0	0	2	2
25	Лекционное занятие 13.	2	0	0	2
26	Лабораторное занятие 13	0	0	2	2
27	Лекционное занятие 14.	2	0	0	2
28	Лабораторное занятие 14	0	0	2	2
29	Лекционное занятие 15.	2	0	0	2
30	Лабораторное занятие 15	0	0	2	2
31	Лекционное занятие 16.	2	0	0	2
32	Лабораторное занятие 16	0	0	2	2

33	Консультация	0	0	0	0
34	Зачет по дисциплине	0	0	0	0
	Часов в 8 семестре	30	0	30	60
	Защита в операционных системах 2	30	0	30	60
1	Лекционное занятие 1.	2	0	0	2
2	Лабораторное занятие 1	0	0	2	2
3	Лекционное занятие 2.	2	0	0	2
4	Лабораторное занятие 2	0	0	2	2
5	Лекционное занятие 3.	2	0	0	2
6	Лабораторное занятие 3	0	0	2	2
7	Лекционное занятие 4.	2	0	0	2
8	Лабораторное занятие 4	0	0	2	2
9	Лекционное занятие 5.	2	0	0	2
10	Лабораторное занятие 5	0	0	2	2
11	Лекционное занятие 6.	2	0	0	2
12	Лабораторное занятие 6	0	0	2	2
13	Лекционное занятие 7.	2	0	0	2
14	Лабораторное занятие 7	0	0	2	2
15	Лекционное занятие 8.	2	0	0	2
16	Лабораторное занятие 8	0	0	2	2
17	Лекционное занятие 9.	2	0	0	2
18	Лабораторное занятие 9	0	0	2	2
19	Лекционное занятие 10.	2	0	0	2
20	Лабораторное занятие 10	0	0	2	2
21	Лекционное занятие 11.	2	0	0	2
22	Лабораторное занятие 11	0	0	2	2
23	Лекционное занятие 12.	2	0	0	2
24	Лабораторное занятие 12	0	0	2	2
25	Лекционное занятие 13.	2	0	0	2
26	Лабораторное занятие 13	0	0	2	2
27	Лекционное занятие 14.	2	0	0	2
28	Лабораторное занятие 14	0	0	2	2
29	Лекционное занятие 15.	2	0	0	2
30	Лабораторное занятие 15	0	0	2	2
31	Консультация	0	0	0	0
32	Консультация	0	0	0	0
33	Экзамен по ЗОС	0	0	0	0
	Итого (ак.часов)	62	0	62	124

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 диф. зачета – 5 семестр, экзамена – 6 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 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: 15.05.2022)

2. 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: 15.05.2022).

3. 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: 15.05.2022).

5.2 Электронные образовательные 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/

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека https://rusneb.ru/

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

MS Office, платформа для электронного обучения Microsoft Teams, ОС MS Windows.

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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора Института
математики и компьютерных наук
М.Н. Перевалова
РАЗРАБОТЧИК(И)
Зулькарнеев И. Р.

ЗАЩИТА ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И ПЕРСОНАЛЬНЫХ ДАННЫХ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность компьютерных систем и сетей» (связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-17*

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.)**
			9
	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. Кин, Э. Ничего личного: Как социальные сети, поисковые системы и спецслужбы используют наши персональные данные / Кин Э. - Москва :Альпина Пабл., 2016. - 224 с.: ISBN 978-5-9614-5128-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/915406 (дата обращения: 10.05.2020). - Режим доступа: по подписке

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.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
И.И. Пряхин

Защита информации от утечки по техническим каналам

Рабочая программа

Специальность: 10.05.01. Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)

форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-4*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Защита информации от утечки по техническим каналам

В результате изучения дисциплины «Технические средства и методы защиты информации» студенты должны:

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;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- пользоваться нормативными документами по защите информации;

владеть:

- навыками работы с нормативными правовыми актами;
- методами и средствами выявления угроз безопасности;
- методами технической защиты информации;
- методами формирования требований по защите информации;
- методами расчета и контроля показателей технической защиты информации;
- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- профессиональной терминологией.
-

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			7
Общая трудоемкость	**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 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 7 семестре	32	0	32	64
	Защита информации от утечки по техническим каналам	32	0	32	64
1	Введение. Характеристика государственной системы противодействия технической разведке	2	0	0	2
2	Обнаружение и локализация источников радиоизлучений	0	0	2	2
3	Нормативные документы по противодействию технической разведке	2	0	0	2
4	Цифровые диктофоны	0	0	2	2
5	Демаскирующие признаки объектов наблюдения и сигналов	2	0	0	2
6	Генераторы радиошума и блокираторы источников радиосигналов	0	0	2	2
7	Средства и методы технической разведки	2	0	0	2
8	Обнаружение и локализация закладных устройств с помощью нелинейного локатора	0	0	2	2
9	Способы и средства перехвата сигналов. Способы и средства наблюдения	2	0	0	2
10	Многофункциональные поисковые приборы, ST-031 «Пиранья»	0	0	2	2
11	Технические каналы утечки информации	2	0	0	2
12	Универсальный анализатор проводных линий «УЛАН-2»	0	0	2	2

13	Оптические и радиоэлектронные каналы утечки информации	2	0	0	2
14	Акустоэлектрические преобразователи	0	0	2	2
15	Акустические и виброакустические каналы утечки информации	2	0	0	2
16	Многофункциональные поисковые приборы, ST-032	0	0	2	2
17	Средства обнаружения технических каналов утечки информации	2	0	0	2
18	Детектор электромагнитного поля ST 007	0	0	2	2
19	Мероприятия по выявлению средств технической разведки	2	0	0	2
20	Принципы дозиметрической разведки. Дозиметрия ионизирующих излучений	0	0	2	2
21	Методы и средства защиты информации от утечки по техническим каналам	2	0	0	2
22	Обнаружение и локализация акустических закладных устройств, программный коррелятор «OSCOR»	0	0	2	2
23	Скрытие речевой информации в каналах связи	2	0	0	2
24	Измерение ПЭМИ монитора и оценка величины зоны R2	0	0	2	2
25	Обнаружение и локализация закладных устройств	2	0	0	2
26	Изучение устройства и работы лазерного микрофона	0	0	2	2
27	Концепция и методы инженернотехнической защиты информации	2	0	0	2
28	Генераторы акустического и виброакустического шума	0	0	2	2
29	Виды контроля и расчёта эффективности защиты информации	2	0	0	2
30	Дополнительная лабораторная работа	0	0	2	2
31	Виды контроля и расчёта эффективности защиты информации	2	0	0	2
32	Дополнительная лабораторная работа	0	0	2	2
33	Консультация	0	0	0	0
34	Экзамен	0	0	0	0
	Итого (ак.часов)	32	0	32	64

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 экзамен (7 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

2. Белоус, А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения : практическое пособие / А. И. Белоус. - Москва ; Вологда : Инфра-Инженерия, 2020. - 644 с. - ISBN 978-5-9729-0512-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167734 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

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: 31.08.2022). – Режим доступа: по подписке.

4. Клименко, И.С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651 (дата обращения: дата обращения: 31.08.2022). – Режим доступа: по подписке.

5. Мосолов, А.С. Компьютерные технологии и методы проектирования в сфере безопасности : учебник для вузов / А. С. Мосолов, Н. И. Акинин. — Санкт-Петербург : Лань, 2021. — 444 с. — ISBN 978-5-8114-8034-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183115 (дата обращения: 31.08.2022). — Режим доступа: для авториз. пользователей.

6. Сычев, Ю.Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:

- Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [Online] (дата обращения: 31.08.2022).

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека. URL: https://rusneb.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.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора Института
математики и компьютерных наук
М.Н. Перевалова
РАЗРАБОТЧИК
Шабалин А. М.

Защита корпоративных сетей
Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01 «Компьютерная безопасность»
Профиль «Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)»
форма обучения очная
Специалитет

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-4.3*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Защита корпоративных сетей

В результате изучения дисциплины студент должен

Знать:

- основы проектирования и работы безопасных коммутируемых сетей;
- организацию и распространение виртуальные локальные сети;
- основы безопасной маршрутизации между сегментами внутри кампусной сети;
- основы безопасности коммутируемых сетей на уровне распределения (distribution);
- основы безопасности коммутируемых сетей на уровне доступа (access);

Уметь:

- настраивать порты коммутатора для подключения WI-FI-точек доступа;
- проектировать и настраивать маршрутизацию между VLAN;
- управлять беспроводным котроллером;
- конфигурировать протоколы FHRP;
- настраивать протоколы класса Spanning Tree;
- применять технологии отказоустойчивости, высокой доступности и мониторинга безопасности компьютерных сетей.

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.**	8	4	4
	час	288	144	144
Из них:				
Часы аудиторной работы (всего):		124	64	60
Лекции		62	32	30
Практические занятия		0	0	0
Лабораторные / практические занятия по подгруппам		62	32	30
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		164	80	84
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный зачет	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 7 семестре	32	0	32	64
	Защита корпоративных сетей	32	0	32	64
1	Лекция 1. Защита программ и данных в компьютерной сети	2	0	0	2
2	Лабораторное занятие 1. Настройка канальных среды в Cisco IOS	0	0	2	2
3	Лекция 2. Дизайн сети предприятия.	2	0	0	2
4	Лабораторное занятие 2. Настройка канальных среды в Huawei VRP	0	0	2	2
5	Лекция 3. Особенности сетевых приложений.	2	0	0	2
6	Лабораторное занятие 3. Policy Base Routing в Cisco IOS	0	0	2	2
7	Лекция 4. Канальные среды.	2	0	0	2
8	Лабораторное занятие 4. Policy Base Routing в Huawei VRP.	0	0	2	2
9	Лекция 5. Маршрутизация в Cisco IOS.	2	0	0	2
10	Лабораторное занятие 5. Static Routing в Cisco IOS	0	0	2	2
11	Лекция 6. CEF. Механизмы манипуляции маршрутной информацией.	2	0	0	2
12	Лабораторное занятие 6. Static Routing в Huawei VRP	0	0	2	2
13	Консультация 1	0	0	0	0
14	Лекция 7. Policy Base Routing.	2	0	0	2
15	Лабораторное занятие 7. RIP в Cisco IOS	0	0	2	2
16	Лекция 8. Статические маршруты для IPv4 / IPv6	2	0	0	2
17	Лабораторное занятие 8. RIP в Huawei VRP	0	0	2	2
18	Лекция 9. Особенности использования статических маршрутов для IPv4 / IPv6	2	0	0	2
19	Лабораторное занятие 9. Конфигурация безопасной работы	0	0	2	2

	протокола EIGRP в классическом (Classic Mode) режиме				
20	Лекция 10. Виды статических маршрутов	2	0	0	2
21	Лабораторное занятие 10. Конфигурация безопасной работы протокола EIGRP в именованном режиме (Named Mode).	0	0	2	2
22	Лекция 11. Варианты применения статических маршрутов для IPv4 / IPv6	2	0	0	2
23	Лабораторное занятие 11. OSPFv2 / OSPFv3 в Cisco IOS	0	0	2	2
24	Консультация 2	0	0	0	0
25	Лекция 12. Защита протокола RIP	2	0	0	2
26	Лабораторное занятие 12. OSPFv2 / OSPFv3 в Huawei VRP	0	0	2	2
27	Лекция 13. EIGRP RTP	2	0	0	2
28	Лабораторное занятие 13. BGP в Cisco IOS.	0	0	2	2
29	Лекция 14. Манипуляции с маршрутами в EIGRP	2	0	0	2
30	Лабораторное занятие 14. Работа с атрибутами BGP в Cisco IOS	0	0	2	2
31	Лекция 15. Расширенный функционал аутентификации в EIGRP Named Mode	2	0	0	2
32	Лабораторное занятие 15. Работа с атрибутами BGP в Huawei VRP	0	0	2	2
33	Лекция 16. Защита протокола OSPF	2	0	0	2
34	Лабораторное занятие 16. Настройка BGP AF-Mode	0	0	2	2
35	Консультация 3	0	0	0	0
36	Зачет по дисциплине	0	0	0	0
	Часов в 8 семестре	30	0	30	60
	Защита корпоративных сетей	30	0	30	60
1	Лекция 1. OSPFv2 LSDB	2	0	0	2
2	Лабораторное занятие 1. DHCPv4 в Cisco IOS	0	0	2	2
3	Лекция 2. Манипуляции с маршрутами в OSPFv2	2	0	0	2
4	Лабораторное занятие 2. DHCPv4 в Huawei VRP	0	0	2	2
5	Лекция 3. Шифрование маршрутной информации IPSEC в протоколе OSPFv3	2	0	0	2
6	Лабораторное занятие 3. DHCPv6 в Cisco IOS	0	0	2	2
7	Лекция 4. Подключение сети предприятия к сети Интернет с использованием протокола BGP	2	0	0	2
8	Лабораторное занятие 4. DHCPv6 в Huawei VRP	0	0	2	2

9	Консультация 1	0	0	0	0
10	Лекция 5. Безопасность сети предприятия в стыках с сетью Интернет	2	0	0	2
11	Лабораторное занятие 5. DNS в Cisco IOS	0	0	2	2
12	Лекция 6. Атрибуты BGP	2	0	0	2
13	Лабораторное занятие 6. DNS в Huawei VRP	0	0	2	2
14	Лекция 7. Защита основных сервисов сети предприятия	2	0	0	2
15	Лабораторное занятие 7. SSH в Cisco IOS	0	0	2	2
16	Консультация 2	0	0	0	0
17	Лекция 8. BGP AF-Mode	2	0	0	2
18	Лабораторное занятие 8. SSH в Huawei VRP	0	0	2	2
19	Лекция 9. Протоколы динамической конфигурации хоста DHCPv4 / DHCPv6	2	0	0	2
20	Лабораторное занятие 9. Настройка автоконфигурации хостов с технологией SLAAC и DHCPv6	0	0	2	2
21	Лекция 10. Служба доменных имен DNS	2	0	0	2
22	Лабораторное занятие 10. TFTP в Cisco IOS	0	0	2	2
23	Лекция 11. Протокол удаленного управления SSH	2	0	0	2
24	Лабораторное занятие 11. TFTP в Huawei VRP	0	0	2	2
25	Консультация 3	0	0	0	0
26	Лекция 12. Защита передаваемых по сети данных	2	0	0	2
27	Лабораторное занятие 12. FTP в Cisco IOS	0	0	2	2
28	Лекция 13. Простой протокол передачи файлов TFTP	2	0	0	2
29	Лабораторное занятие 13. FTP в Huawei VRP	0	0	2	2
30	Лекция 14. Аутентификация и авторизация в протоколе FTP	2	0	0	2
31	Лабораторное занятие 14. SCP в Cisco IOS	0	0	2	2
32	Лекция 15. Шифрование трафика протоколом SCP	2	0	0	2
33	Лабораторное занятие 15. SCP в Huawei VRP	0	0	2	2
34	Консультация 4	0	0	0	0
35	Экзамен	0	0	0	0
	Итого (ак.часов)	62	0	62	124

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 диф. зачета в 7 семестре, в форме экзамена в 8 семестре.

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. 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.
2. 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.
3. 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.
4. 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.

5.2 Электронные образовательные ресурсы:

– MITRE ATT&CK. https://attack.mitre.org/
– Банк данных угроз безопасности информации. https://bdu.fstec.ru/vul

6. 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/

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

- MS Windows 10
- MS Office,

- Oracle Virtual Box
- GNS3
- платформа для электронного обучения Microsoft Teams.

8. Технические средства и материально-техническое обеспечение дисциплины

Мультимедийная учебная аудитория для проведения занятий лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

Компьютерный класс с выходом в интернет.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместителем директора
института Переваловой М.Н.
РАЗРАБОТЧИК(И)
Оленников Е.А.

Компьютерная форензика и расследование инцидентов

Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01. Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ОПК-6

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

В результате освоения дисциплины обучающиеся будут
Знать:

- о компьютерной криминалистике и правовом обеспечении расследования инцидентов информационной безопасности;
- об анализе лог-файлов;
- об алгоритме расследования инцидентов информационной безопасности;
- о производстве компьютерно-технической экспертизы;
- об основных программных и аппаратных средствах поиска уликовых данных;
- о вскрытии защищенных данных, хранящихся в специализированных «контейнерах», запароленных архивах и т.п.;

Уметь:

- искать утраченную или сокрытую информацию на компьютере и мобильных устройствах;
- документально оформлять процесс расследования инцидентов ИБ;
- документально оформлять процесс проведения компьютерно-технической экспертизы

Владеть:

- навыками расследование инцидентов информационной безопасности;
- навыками производства компьютерно-технической экспертизы;
- навыками работы со специализированным программным и аппаратным обеспечением по проведению компьютерно-технической экспертизы.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			10
Общая трудоемкость	**зач. ед.**	4	4
	час	144	144
Из них:			
Часы аудиторной работы (всего):		60	60
Лекции		30	30
Практические занятия		0	0
Лабораторные / практические занятия по подгруппам		30	30
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		84	84
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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 10 семестре	30	0	30	60
	Компьютерная форензика и расследование инцидентов	30	0	30	60
1	Введение в уголовно-правовое обеспечение ИБ	2	0	0	2
2	Знакомство с оборудованием	0	0	2	2
3	Преступления в информационной сфере	2	0	0	2
4	Обучающая игра	0	0	2	2
5	Компьютерные преступления	2	0	0	2
6	Работа с объектом исследований	0	0	2	2
7	Изъятие и подготовка объекта исследований	2	0	0	2
8	Изъятие и подготовка объекта исследований	0	0	2	2
9	Инструментарий компьютерной криминалистики	2	0	0	2
10	Изъятие и подготовка объекта исследований	0	0	2	2
11	Расследование инцидентов информационной безопасности	2	0	0	2
12	Оформление инцидента ИБ	0	0	2	2
13	Работа с лог-файлами	2	0	0	2
14	Работа с лог-файлами	0	0	2	2
15	Правовые основы производства экспертиз	2	0	0	2
16	Основные документы для проведения экспертиз	0	0	2	2
17	Производство компьютерно-технической экспертизы	2	0	0	2
18	Документы компьютерно-технической экспертизы	0	0	2	2
19	Поиск уликовой информации на компьютерах	2	0	0	2

20	Поиск уликовой информации на компьютерах	0	0	2	2
21	Артефакты ОС Windows.	2	0	0	2
22	Артефакты ОС Windows	0	0	2	2
23	Исследование дампов оперативной памяти	2	0	0	2
24	Исследование дампов оперативной памяти	0	0	2	2
25	Работа с системами поиска остаточной информации	2	0	0	2
26	Работа с системами поиска остаточной информации	0	0	2	2
27	Поиск сообщений электронной почты	2	0	0	2
28	Поиск сообщений электронной почты	0	0	2	2
29	Работа с криптографией. Работа с мобильными устройствами.	2	0	0	2
30	Работа с криптографией. Работа с мобильными устройствами.	0	0	2	2
31	Консультация	0	0	0	0
32	Зачет	0	0	0	0
	Итого (ак.часов)	30	0	30	60

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 диф. 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Грачев, Я. Л. Анализ изображений с точки зрения компьютерной криминалистики (Стегоанализ изображений) : учебное пособие / Я. Л. Грачев, В. Г. Сидоренко. — Москва : Российский университет транспорта (МИИТ), 2021. — 84 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/122048.html (дата обращения: 23.11.2022).

2. Калмыков, И. А. Компьютерная криминалистика : лабораторный практикум / И. А. Калмыков, В. С. Пелешенко. — Ставрополь : Северо-Кавказский федеральный университет, 2017. — 84 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/69392.html (дата обращения: 23.11.2022).

5.2 Электронные образовательные 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.

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека https://rusneb.ru/

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

MS Office, платформа для электронного обучения Microsoft Teams, ОС MS Windows, ОС FreeBSD.

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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска

аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМКН
Перевалова М.Н.
РАЗРАБОТЧИК(И)
Ниссенбаум О.В.

Криптографические протоколы

Рабочая программа
для обучающихся по специальности 10.05.01. Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
Уровень высшего образования: специалитет
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ОПК-10

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Криптографические протоколы

Знать:

- основные типы криптографических протоколов и их свойства;
- криптографические стандарты;
- типовые криптографические протоколы и основные требования к ним;
- основные схемы цифровой подписи;
- протоколы идентификации;
- протоколы передачи и распределения ключей;

уметь:

- использовать симметричные и асимметричные шифры системы для построения криптографических протоколов;
- формулировать свойства безопасности криптографических протоколов;
- проводить сравнительный анализ криптографических протоколов, решающих сходные задачи;

владеть:

- криптографической терминологией;
- навыками программной реализации криптографических протоколов;
- навыками оценки эффективности протокола;
- способностью читать и понимать научную и инженерно-техническую литературу по криптографическим протоколам, в том числе на английском языке;
- простейшими подходами к анализу безопасности криптографических протоколов.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			8
Общая трудоемкость	**зач. ед.**	4	4
	час	144	144
Из них:			
Часы аудиторной работы (всего):		60	60
Лекции		30	30
Практические занятия		30	30
Лабораторные / практические занятия по подгруппам		0	0

Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося	84	84
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)		Дифференцированный 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 8 семестре	30	30	0	60
	Криптографические протоколы	30	30	0	60
1	Введение в криптографические протоколы	2	0	0	2
2	Введение в криптографические протоколы	0	2	0	2
3	Цифровые подписи общего назначения	2	0	0	2
4	Цифровые подписи общего назначения.	0	2	0	2
5	Эллиптические кривые.	2	0	0	2
6	Эллиптические кривые.	0	2	0	2
7	Цифровые подписи на эллиптической кривой.	2	0	0	2
8	Цифровые подписи на эллиптической кривой.	0	2	0	2
9	Цифровые подписи специального назначения. Коллективная подпись. Слепая подпись.	2	0	0	2
10	Цифровые подписи специального назначения.	0	2	0	2
11	Цифровые подписи специального назначения. Подпись со скрытым каналом. Неотрицаемая подпись.	2	0	0	2
12	Свойства цифровых подписей.	0	2	0	2
13	Привязка к биту и электронная жеребьевка.	2	0	0	2
14	Электронная жеребьевка.	0	2	0	2
15	Разделение секрета.	2	0	0	2
16	Разделение секрета.	0	2	0	2
17	Конфиденциальные вычисления.	2	0	0	2
18	Конфиденциальные вычисления.	0	2	0	2
19	Покер по телефону.	2	0	0	2
20	Покер по телефону.	0	2	0	2
21	Идентификация и аутентификация.	2	0	0	2

22	Идентификация и аутентификация.	0	2	0	2
23	Протоколы идентификации с нулевым разглашением.	2	0	0	2
24	Управление ключами.	0	2	0	2
25	Электронная монета.	2	0	0	2
26	Электронная монета.	0	2	0	2
27	Управление ключами.	2	0	0	2
28	Электронные выборы.	0	2	0	2
29	Инфраструктура открытых ключей. Прикладные сетевые протоколы.	2	0	0	2
30	Прикладные сетевые протоколы	0	2	0	2
31	Консультация	0	0	0	0
32	Консультация	0	0	0	0
33	Дифференцированный зачет	0	0	0	0
	Итого (ак.часов)	30	30	0	60

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 устного дифференцированного зачета.

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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

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 (30.10.2022)

2. Криптографические методы защиты информации. Том 3: Учебно-методическое 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 (30.10.2022)

Дополнительная литература:

1. Ниссенбаум, О. В. Криптографические протоколы: лабораторный практикум: учебно-методическое пособие для студентов специальностей "Компьютерная безопасность" и "Информационная безопасность автоматизированных систем"/ О.В. Ниссенбаум, Н.В. Поляков; Тюм. гос. ун-т. - Тюмень: Изд-во ТюмГУ, 2012. - 40 с.

2. Торстейнсон, П. Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г.А. Ганеш; пер. с англ. - 2-е изд. (эл.). - М.: БИНОМ. Лаборатория знаний, 2013. - 480 с.: ил. - (Программисту). - ISBN 978-5-9963-1345- 7. - Режим доступа: http://znanium.com/catalog/product/478090 (30.10.2022)

3. Введение в криптографию. Курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — М.: ФОРУМ: ИНФРА-М, 2018. — 240 с. — (Высшее образование: Бакалавриат). [Электронный ресурс] – URL: http://znanium.com/catalog/product/924700 (30.10.2022)

5.2 Электронные образовательные 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.

6. Современные профессиональные базы данных и информационные справочные системы:

- http://www.iacr.org – ресурс Международной ассоциации криптографических исследований

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

MS Office, платформа для электронного обучения Microsoft Teams.
Visual Studio или другая IDE

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 семинарского типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная.

Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, персональные компьютеры.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
Т.И. Паюсова

МЕТОДЫ И СРЕДСТВА ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01. Компьютерная безопасность
специализация Безопасность компьютерных систем и сетей
(связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-8*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Знать:
1) Основные направления применения искусственного интеллекта в информационной безопасности;
2) Типы задач машинного обучения;
3) Основные алгоритмы моделей машинного обучения.

Уметь:
1) Выбирать модели МО для решения задач ИБ;
2) Применять программные инструменты и библиотеки для решения задач ИБ с помощью методов МО;
3) Формировать датасеты для обучения моделей МО;
4) Оценивать качество моделей МО.

Владеть:
1) Навыками построения и обучения моделей МО на языке Python с использованием библиотек NumPy, Keras, Tensorflow, Scikit-learn и др.
2) Навыками формирования датасетов для машинного обучения (разметка текстов, нормализация, стемминг, кодирование и пр.)
3) Навыками оценки качества моделей машинного обучения с помощью метрик (матрицы ошибок (confusion matrix), accuracy, precision, recall, F-меры, AUC-ROC и др.).

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			10
Общая трудоемкость	**зач. ед.**	4	4
	час	144	144
Из них:			
Часы аудиторной работы (всего):		60	60
Лекции		30	30
Практические занятия		30	30
Лабораторные / практические занятия по подгруппам		0	0
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		84	84
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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 10 семестре	30	30	0	60
	Методы и средства искусственного интеллекта в информационной безопасности	30	30	0	60
1	**Лекционное занятие 1** Обзор наиболее актуальных задач ИБ, решение которых предполагает применение методов машинного обучения (задачи компьютерного зрения и машинного слуха, обнаружения аномалий в сетевой активности, прогнозирование атак и др.).	2	0	0	2
2	**Практическое занятие 1** Знакомство с программными инструментами и библиотеками для решения задач ИБ с помощью методов МО (NumPy, Keras, Tensorflow, Scikit-learn и др.).	0	2	0	2
3	**Самостоятельная работа** Чтение основной и дополнительной литературы, работа с конспектом лекции.	0	0	0	0
4	**Лекционное занятие 2** Задачи машинного обучения (классификации, кластеризации, восстановления регрессии, поиска ассоциативных правил и пр.).	2	0	0	2
5	**Практическое занятие 2** Обзор датасетов по ИБ для обучения моделей МО (Netresec (PCAP), KDD Cup 1999, Web Attack Payloads, DARPA IDS Dataset, Stratosphere IPS Dataset, Aktaion (Bro, phishing, ransomware и др.), Malicious URL	0	2	0	2

	Dataset (Sysnet), Malware Training set, Ember (для malware), NSA CDX).				
6	**Самостоятельная работа** Чтение основной и дополнительной литературы, работа с конспектом лекции.	0	0	0	0
7	**Лекционное занятие 3** Обзор атак на модели МО (DeepFool, One pixel, FGSM, JSMA, Adversarial атака и др.)	2	0	0	2
8	**Практическое занятие 3** Подготовка среды PyCharm, установка необходимых для дальнейшей работы библиотек, проверка настроек.	0	2	0	2
9	**Самостоятельная работа** Чтение основной и дополнительной литературы, работа с конспектом лекции.	0	0	0	0
10	**Лекционное занятие 4** Обзор методов защиты от атак на модели МО (анализ дифференцированного воздействия, обнаружение аномалий, валидация входных данных, RONI (Reject on negative impact), KNHT (Keyed Non-parametric Hypothesis Tests), контроль версий и пр.).	2	0	0	2
11	**Практическое занятие 4** Знакомство с библиотекой OpenCV (применение модулей для выполнения математических операций, обработки изображений и видео, 3D-моделирования).	0	2	0	2
12	**Самостоятельная работа** Чтение основной и дополнительной литературы, работа с конспектом лекции.	0	0	0	0
13	**Лекционное занятие 5** Основные задачи МО: задача классификации, кластеризации, восстановления регрессии, поиска ассоциативных правил.	2	0	0	2
14	**Практическое занятие 5** Построение классификатора для обнаружения вторжений и распознавания атак на основе набора данных KDD99 (описание и постановка задачи).	0	2	0	2
15	**Самостоятельная работа** Чтение основной и дополнительной литературы, работа с конспектом лекции.	0	0	0	0

16	**Лекционное занятие 6** Обзор основных методов решения задач МО: дерево принятия решений, метод наименьших квадратов, метод опорных векторов, искусственные нейронные сети.	2	0	0	2
17	**Практическое занятие 6** Построение классификатора для обнаружения вторжений и распознавания атак на основе набора данных KDD99 (реализация и сравнительный анализ результатов на базе алгоритмов K-NN, SVDD, OCSVM).	0	2	0	2
18	**Самостоятельная работа** Чтение основной и дополнительной литературы, работа с конспектом лекции.	0	0	0	0
19	**Лекционное занятие 7** Введение в теорию искусственных нейронных сетей.	2	0	0	2
20	**Практическое занятие 7** Обзор основных функций и возможностей библиотек TensorFlow, Keras, NumPy.	0	2	0	2
21	**Самостоятельная работа** Чтение основной и дополнительной литературы, работа с конспектом лекции.	0	0	0	0
22	**Лекционное занятие 8** Анализ и оценка качества обучения нейронной сети с помощью метрик. Понятия обучающей, проверочной и тестовой выборок. Проблема переобучения модели.	2	0	0	2
23	**Практическое занятие 8** Реализация многослойного перцептрона с помощью библиотек TensorFlow, Keras, NumPy для решения задачи аутентификации субъекта по подписи.	0	2	0	2
24	**Самостоятельная работа** Чтение основной и дополнительной литературы, работа с конспектом лекции.	0	0	0	0
25	**Лекционное занятие 9** Градиентный спуск. Алгоритм обратного распространения ошибки.	2	0	0	2
26	**Практическое занятие 9** Обучение построенной нейросетевой модели с помощью алгоритма обратного распространения ошибки.	0	2	0	2

27	**Самостоятельная работа** Чтение основной и дополнительной литературы, работа с конспектом лекции.	0	0	0	0
28	**Лекционное занятие 10** Свёрточные нейронные сети (CNN). Задача распознавания изображений.	2	0	0	2
29	**Практическое занятие 10** Реализация и обучение свёрточной нейросети на базе датасета CIFAR-10.	0	2	0	2
30	**Самостоятельная работа** Чтение основной и дополнительной литературы, работа с конспектом лекции.	0	0	0	0
31	**Лекционное занятие 11** Знакомство с генеративно-состязательными сетями (GAN), функциями активации ReLU и Leaky ReLU.	2	0	0	2
32	**Практическое занятие 11** Реализация задачи аутентификации субъектов по геометрии лица с помощью генеративно-состязательной нейросети.	0	2	0	2
33	**Лекционное занятие 12** Аспекты формирования наборов данных для машинного обучения (разметка текстов, нормализация, стемминг, кодирование и пр.)	2	0	0	2
34	**Практическое занятие 12** Работа с библиотеками beautifulsoup4, lxml, NLTK, scikit-learn, wordcloud, Gensim, pymorphy2 для обработки текстового контента.	0	2	0	2
35	**Лекционное занятие 13** Задача машинного слуха. Аутентификация по голосу. Определение значимых характеристик голоса. Оптимизация алгоритма с помощью фильтров тишины и пауз.	2	0	0	2
36	**Практическое занятие 13** Реализация задачи аутентификации человека по голосу с помощью нейросетевой модели и библиотек Keras, Librosa, NumPy.	0	2	0	2
37	**Лекционное занятие 14** Совершенствование процессов обнаружения и предотвращения вторжений с помощью МО.	2	0	0	2
38	**Практическое занятие 14** Реализация нейросетевого модуля для системы обнаружения вторжений	0	2	0	2

	(IDS) Snort (детектирование сетевых атак).				
39	**Лекционное занятие 15** Прогнозирование атак и проактивный поиск угроз (Threat Hunting) с помощью машинного обучения.	2	0	0	2
40	**Практическое занятие 15** Формирование Red Team сценария атак с помощью нейросетевого моделирования на базе MITRE ATTA&CK, IoC, CVE, CAR, SHIELD Active Defense, Darknet-контента.	0	2	0	2
41	Консультация	0	0	0	0
42	Дифференцированный зачет	0	0	0	0
	Итого (ак.часов)	30	30	0	60

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 дифференцированный зачет (10 семестр).

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:

Основная литература

1. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

2. Келлехер, Д. Наука о данных: базовый курс / Джон Келлехер, Брендан Тирни ; пер. с англ.. - Москва : Альпина Паблишер, 2020. - 222 с. - ISBN 978-5-9614-3170-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1221800 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

3. Клименко, И.С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651 (дата обращения: дата обращения: 31.08.2022). – Режим доступа: по подписке.

4. Протодьяконов, А. В. Алгоритмы Data Science и их практическая реализация на Python : учебное пособие / А. В. Протодьяконов, П. А. Пылов, В. Е. Садовников. - Москва ; Вологда : Инфра-Инженерия, 2022. - 392 с. - ISBN 978-5-9729-1006-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902689 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Бруссард, М. Искусственный интеллект: пределы возможного / Мередит Бруссард ; пер. с англ. - Москва : Альпина нон-фикшн, 2020. - 362 с. - ISBN 978-5-00139-080-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1220958 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

2. Одинцов, Б. Е. Модели и проблемы интеллектуальных систем : монография / Б.Е. Одинцов. — Москва : ИНФРА-М, 2020. — 219 с. — (Научная мысль). — DOI 10.12737/1060845. - ISBN 978-5-16-015839-6. - Текст : электронный. - URL:

https://znanium.com/catalog/product/1060845 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:

- Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [On-line] (дата обращения: 31.08.2022).

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека. URL: https://rusneb.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.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМКН
Перевалова М.Н.
РАЗРАБОТЧИК(И)
Ниссенбаум О.В.

етоды и средства криптографической защиты информации

Рабочая программа
для обучающихся по специальности 10.05.01. Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
Уровень высшего образования: специалитет
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-10*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Методы и средства криптографической защиты информации

знать:

- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- модели шифров и математические методы их исследования;
- принципы построения криптографических алгоритмов;
- криптографические стандарты;
- использование криптографических стандартах в информационных системах;
- о системах криптографической защиты информации (СКЗИ).

уметь:

- применять криптографические алгоритмы на практике;
- применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- осуществлять программную реализацию криптографических алгоритмов;
- пользоваться научно-технической литературой в области криптографии;

владеть:

- криптографической терминологией;
- навыками программной реализации криптографических алгоритмов;
- навыками использования типовых криптографических алгоритмов;
- навыками использования ПЭВМ в анализе простейших шифров;
- навыками математического моделирования в криптографии;
- средствами обеспечения информационной безопасности;
- навыками определения видов и форм информации, подверженных угрозам и возможных методов и путей устранения этих угроз.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			8
Общая трудоемкость	**зач. ед.**	4	4
	час	144	144
Из них:			
Часы аудиторной работы (всего):		60	60
Лекции		30	30

Практические занятия	30	30
Лабораторные / практические занятия по подгруппам	0	0
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося	84	84
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)		Дифференцированный 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 8 семестре	30	30	0	60
	Методы и средства криптографической защиты информации	30	30	0	60
1	Введение в криптографию.	2	0	0	2
2	Исторические шифры	0	2	0	2
3	Исторические шифры	2	0	0	2
4	Криптоанализ исторических шифров	0	2	0	2
5	Исторические шифры	2	0	0	2
6	Раундовое преобразование шифра "Магма"	0	2	0	2
7	Математическая модель шифра.	2	0	0	2
8	Шифр ГОСТ Р 34.12-2015	0	2	0	2
9	Блочные шифры.	2	0	0	2
10	Консультация	0	0	0	0
11	Режимы ГОСТ Р 34.13-2015.	0	2	0	2
12	Режимы блочного шифрования	2	0	0	2
13	Операции с многочленами над Z2	0	2	0	2
14	Поля Галуа.	2	0	0	2
15	Элементарные преобразования XLPS-шифра	0	2	0	2
16	Математика XLPS-шифров.	2	0	0	2
17	XLPS-шифры	0	2	0	2
18	Шифр SQUARE	2	0	0	2
19	Теория секретности Шеннона	0	2	0	2
20	Шифры AES и ГОСТ Р 34.12-2015 "Кузнечик"	2	0	0	2
21	Консультация	0	0	0	0
22	Регистры сдвига с линейной обратной связью и генераторы ПСГ на их основе.	0	2	0	2
23	Многократное шифрование	2	0	0	2
24	Хэш-функции на основе блочных преобразований.	0	2	0	2

25	Теория секретности Шеннона	2	0	0	2
26	Стандарты на хэш-функции	0	2	0	2
27	Поточные шифры	2	0	0	2
28	Коды аутентификации сообщений	0	2	0	2
29	Поточные генераторы и шифры.	2	0	0	2
30	Тесты на простоту	0	2	0	2
31	Теория имитостойкости Симмонса. Понятие ЗКС и хэш-функции.	2	0	0	2
32	Асимметричные шифры и цифровая подпись	0	2	0	2
33	Консультация перед экзаменом	0	0	0	0
34	Консультация	0	0	0	0
35	Дифференцированный зачет	0	0	0	0
	Итого (ак.часов)	30	30	0	60

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 *устного дифференцированного зачета.*

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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

Основная литература:

1. Криптографические методы защиты информации. Том 3: Учебно-методическое 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 (30.10.2022).

2. 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: 27 https://doi.org/10.12737/1716-6 [Электронный ресурс]. - URL: http://znanium.com/catalog/product/901659 (30.10.2022).

3. Введение в криптографию. Курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — М.: ФОРУМ: ИНФРА-М, 2018. — 240 с. — (Высшее образование: Бакалавриат). [Электронный ресурс]. – URL: http://znanium.com/catalog/product/924700 (30.10.2022).

Дополнительная литература:

1. Безопасность и управление доступом в информационных системах: учеб. пособие / А.В. Васильков, И.А. Васильков. — М.: ФОРУМ: ИНФРА-М, 2017. — 368 с. — Режим доступа: http://znanium.com/catalog/product/537054 (дата обращения: 30.10.2022).

2. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс]: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск: Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. – Режим доступа: http://znanium.com/catalog/product/441493 (дата обращения: 30.10.2022).

5.2 Электронные образовательные 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.

6. Современные профессиональные базы данных и информационные справочные системы:

- http://www.iacr.org – ресурс Международной ассоциации криптографических исследований

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

MS Office, платформа для электронного обучения Microsoft Teams.
Visual Studio или другая IDE

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 семинарского типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная.

Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, персональные компьютеры.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
Т.И. Паюсова

Методы оценки безопасности компьютерных систем и сетей (пентестинг)

Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01. Компьютерная безопасность
специализация Безопасность компьютерных систем и сетей
(связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-15*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Методы оценки безопасности компьютерных систем и сетей (пентестинг)

Знать:

1) различные подходы к организации процесса проверки подлинности сущностей информационной безопасности;

2) особенности моделей разграничения прав доступа в информационной системе;

3) способы учитывать и анализировать действия пользователей в информационной системе;

4) методики проведения аудита информационной безопасности и теста на проникновение;

Уметь:

1) реализовывать различные методы проверки подлинности сущностей информационной безопасности;

2) адекватно применять ту или иную модель разграничения прав доступа;

3) учитывать и анализировать действия пользователей в информационной системе программными методами;

4) проводить аудит информационной безопасности и тест на проникновение;

Владеть:

1) навыками реализации различных подходов к проверке подлинности сущностей информационной безопасности;

2) навыками адекватного применения и реализации различных моделей разграничения прав доступа;

3) навыками построения системы учета и анализа действия пользователей в информационной системе;

4) навыками организации и проведения аудита информационной безопасности и теста на проникновение.

Компетенции:

ИБ:

Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности (ОПК-2);

КБ:

Способен администрировать компьютерные сети и контролировать корректность их функционирования (ОПК-15).

Шкала перевода рейтинговых баллов в оценку:

от 91 до 100 баллов - отлично;
от 76 до 90 баллов - хорошо;
от 61 до 75 баллов - удовлетворительно;
менее 61 балла - неудовлетворительно.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			9
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося		80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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	32	0	32	64
	Методы оценки безопасности компьютерных систем и сетей (пентестинг)	32	0	32	64
1	Тема №1. Введение в пентестинг	4	0	0	4
2	Знакомство с дорожной картой пентестера	0	0	4	4
3	Тема №2. Базовый арсенал пентестера	4	0	0	4
4	Стандартный набор инструментов пентестера	0	0	4	4
5	Тема №3. Уязвимости информационной системы	4	0	0	4
6	Поиск и анализ уязвимостей системы	0	0	4	4
7	Тема №4. Обзор нормативно-правовой и законодательной базы ИБ	4	0	0	4
8	Знакомство с основными законами и нормативно-правовыми актами в области информационной безопасности	0	0	4	4
9	Тема №5. Базовая система защиты информации	4	0	0	4
10	Базовая система защиты информации	0	0	4	4
11	Тема №6. Базовый тест на проникновение в информационную систему	4	0	0	4
12	Проведение базового теста на проникновения в информационную систему	0	0	4	4
13	Тема №7. Документация при проведении тестов на проникновение	4	0	0	4
14	Пакет документов для проведения тестирования на проникновение	0	0	4	4
15	Тема №8. Сертификация в области пентеста	4	0	0	4
16	Сертификация в области пентестинга	0	0	4	4

17	Консультация	0	0	0	0
18	Дифференцированный зачет	0	0	0	0
	Итого (ак.часов)	32	0	32	64

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 дифференцированный зачет (9 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вешах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

2. Белоус, А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения : практическое пособие / А. И. Белоус. - Москва ; Вологда : Инфра-Инженерия, 2020. - 644 с. - ISBN 978-5-9729-0512-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167734 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

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: 31.08.2022). – Режим доступа: по подписке.

4. Клименко, И.С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651 (дата обращения: дата обращения: 31.08.2022). – Режим доступа: по подписке.

5. Мосолов, А.С. Компьютерные технологии и методы проектирования в сфере безопасности : учебник для вузов / А. С. Мосолов, Н. И. Акинин. — Санкт-Петербург : Лань, 2021. — 444 с. — ISBN 978-5-8114-8034-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183115 (дата обращения: 31.08.2022). — Режим доступа: для авториз. пользователей.

6. Сычев, Ю.Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование:

Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:

- Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [On-line] (дата обращения: 31.08.2022).

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека. URL: https://rusneb.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.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
Т.И. Паюсова

МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01. Компьютерная безопасность
специализация Безопасность компьютерных систем и сетей
(связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-11*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Перечень планируемых результатов обучения по дисциплине (модулю):
Знать:

- основные модели доступа в информационной системе;
- методы формального описания модели злоумышленника;
- основные способы формального описания и анализа политик безопасности;
- методы анализа модели угроз.

Уметь:

- реализовывать основные модели доступа в информационной системе;
- формально описывать модель злоумышленника;
- формально описывать и анализировать политику безопасности;
- анализировать модель угроз.

Владеть:

- навыками реализации основных моделей доступа в информационной системе;
- навыками формального описания модели злоумышленника;
- навыками формального описания и анализа политик безопасности;
- навыками анализа модели угроз.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			6
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося		80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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 6 семестре	32	32	0	64
	Модели безопасности компьютерных систем	32	32	0	64
1	Тема 1. Введение в теоретический подход к обеспечению информационной безопасности	2	0	0	2
2	Тема 1. Математические основы построения моделей безопасности	0	2	0	2
3	Самостоятельная работа по Теме 1. Введение в теоретический подход к обеспечению информационной безопасности	0	0	0	0
4	Тема 1. Введение в теоретический подход к обеспечению информационной безопасности	2	0	0	2
5	Тема 1. Математические основы построения моделей безопасности	0	2	0	2
6	Самостоятельная работа по Теме 1. Введение в теоретический подход к обеспечению информационной безопасности	0	0	0	0
7	Тема 2. Математические основы построения моделей безопасности	2	0	0	2
8	Тема 2. Математические основы построения моделей безопасности	0	2	0	2
9	Самостоятельная работа по Теме 2. Математические основы построения моделей безопасности	0	0	0	0
10	Тема 2. Математические основы построения моделей безопасности	2	0	0	2
11	Тема 2. Математические основы построения моделей безопасности	0	2	0	2
12	Самостоятельная работа по Теме 2. Математические основы построения моделей безопасности	0	0	0	0

13	Тема 3. Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU)	2	0	0	2
14	Тема 3. Математические основы построения моделей безопасности	0	2	0	2
15	Самостоятельная работа по Теме 3. Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU)	0	0	0	0
16	Тема 3. Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU)	2	0	0	2
17	Тема 3. Математические основы построения моделей безопасности	0	2	0	2
18	Самостоятельная работа по Теме 3. Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU)	0	0	0	0
19	Тема 4. Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД)	2	0	0	2
20	Тема 4. Дискреционная модель доступа	0	2	0	2
21	Самостоятельная работа по Теме 4. Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД)	0	0	0	0
22	Тема 4. Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД)	2	0	0	2
23	Тема 4. Дискреционная модель доступа	0	2	0	2
24	Самостоятельная работа по Теме 4. Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД)	0	0	0	0
25	Тема 5. Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant	2	0	0	2
26	Тема 5. Дискреционная модель доступа	0	2	0	2
27	Самостоятельная работа по Теме 5. Модели компьютерных систем с	0	0	0	0

	дискреционным управлением. Модель распространения прав доступа Take-Grant				
28	Тема 5. Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant	2	0	0	2
29	Тема 5. Дискреционная модель доступа	0	2	0	2
30	Самостоятельная работа по Теме 5. Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant	0	0	0	0
31	Тема 6. Модели компьютерных систем с мандатным управлением. Модель Белла-ЛаПадулы	2	0	0	2
32	Тема 6. Мандатная модель доступа	0	2	0	2
33	Самостоятельная работа по Теме 6. Модели компьютерных систем с мандатным управлением. Модель Белла-ЛаПадулы	0	0	0	0
34	Тема 6. Модели компьютерных систем с мандатным управлением. Модель Белла-ЛаПадулы	2	0	0	2
35	Тема 6. Мандатная модель доступа	0	2	0	2
36	Самостоятельная работа по Теме 6. Модели компьютерных систем с мандатным управлением. Модель Белла-ЛаПадулы	0	0	0	0
37	Тема 7. Модели компьютерных систем с мандатным управлением. Модель Биба. Модель систем военных сообщений	2	0	0	2
38	Тема 7. Ролевая модель доступа	0	2	0	2
39	Самостоятельная работа по Теме 7. Модели компьютерных систем с мандатным управлением. Модель Биба. Модель систем военных сообщений	0	0	0	0
40	Тема 7. Модели компьютерных систем с мандатным управлением. Модель Биба. Модель систем военных сообщений	2	0	0	2
41	Тема 7. Ролевая модель доступа	0	2	0	2
42	Самостоятельная работа по Теме 7. Модели компьютерных систем с мандатным управлением. Модель Биба. Модель систем военных сообщений	0	0	0	0
43	Тема 8. Модели компьютерных систем с ролевым управлением	2	0	0	2

44	Тема 8. Атрибутивная модель доступа	0	2	0	2
45	Самостоятельная работа по Теме 8. Модели компьютерных систем с ролевым управлением	0	0	0	0
46	Тема 9. Модели безопасности информационных потоков и изолированной программной среды	2	0	0	2
47	Тема 9. Модели безопасности информационных потоков и изолированной программной среды	0	2	0	2
48	Самостоятельная работа по Теме 9. Модели безопасности информационных потоков и изолированной программной среды	0	0	0	0
49	Консультация	0	0	0	0
50	Дифференцированный зачет	0	0	0	0
	Итого (ак.часов)	32	32	0	64

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 дифференцированный зачет (6 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вешах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

2. Белоус, А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения : практическое пособие / А. И. Белоус. - Москва ; Вологда : Инфра-Инженерия, 2020. - 644 с. - ISBN 978-5-9729-0512-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167734 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

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: 31.08.2022). – Режим доступа: по подписке.

4. Клименко, И.С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651 (дата обращения: дата обращения: 31.08.2022). – Режим доступа: по подписке.

5. Мосолов, А.С. Компьютерные технологии и методы проектирования в сфере безопасности : учебник для вузов / А. С. Мосолов, Н. И. Акинин. — Санкт-Петербург : Лань, 2021. — 444 с. — ISBN 978-5-8114-8034-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183115 (дата обращения: 31.08.2022). — Режим доступа: для авториз. пользователей.

6. Сычев, Ю.Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование:

Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:

- Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [On-line] (дата обращения: 31.08.2022).

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека. URL: https://rusneb.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.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора Института
математики и компьютерных наук
М.Н. Перевалова
РАЗРАБОТЧИК(И)
Зулькарнеев И. Р.

Научно-проектный (исследовательский) семинар
Рабочая программа
10.05.01 «Компьютерная безопасность»
специализация «Безопасность компьютерных систем и сетей» (связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* УК-1,2,3,4,5,6,9

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	11
Общая трудоемкость	**зач. ед.**	8	4	4
	час	288	144	144
Из них:				
Часы аудиторной работы (всего):		36	18	18
Лекции		16	8	8
Практические занятия		20	10	10
Лабораторные / практические занятия по подгруппам		0	0	0
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		252	126	126
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный зачет	Дифференцированный 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 11 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 11 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: 24.11.2022). — 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.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместителем директора
института Переваловой М.Н.
РАЗРАБОТЧИК(И)
Оленников Е. А.

Операционные системы специального назначения

Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01. Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ОПК-12.

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Знания:

- основные ЗОС;
- назначение, характеристики, особенности ЗОС;
- задачи, решаемые с помощью ЗОС;
- архитектуру ЗОС;
- основные модели управления доступом, применяемые в ЗОС;
- основные задачи по конфигурированию и администрированию ЗОС;
- встроенные сервисы безопасности ЗОС;

подходы к управлению безопасностью в ЗОС.

Умения:

- выполнять установку и конфигурирование ЗОС;
- конфигурировать сервисы безопасности ЗОС;
- администрировать ЗОС.

Навыки:

- пользовательской работы в ЗОС;
- базового администрирования ЗОС.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			9
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося		80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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 9 семестре	32	0	32	64
1	Лекционное занятие 1.	2	0	0	2
2	Лабораторное занятие 1	0	0	2	2
3	Лекционное занятие 2.	2	0	0	2
4	Лабораторное занятие 2	0	0	2	2
5	Лекционное занятие 3.	2	0	0	2
6	Лабораторное занятие 3	0	0	2	2
7	Лекционное занятие 4.	2	0	0	2
8	Лабораторное занятие 4	0	0	2	2
9	Лекционное занятие 5.	2	0	0	2
10	Лабораторное занятие 5	0	0	2	2
11	Лекционное занятие 6.	2	0	0	2
12	Лабораторное занятие 6	0	0	2	2
13	Лекционное занятие 7.	2	0	0	2
14	Лабораторное занятие 7	0	0	2	2
15	Лекционное занятие 8.	2	0	0	2
16	Лабораторное занятие 8	0	0	2	2
17	Лекционное занятие 9.	2	0	0	2
18	Лабораторное занятие 9	0	0	2	2
19	Лекционное занятие 10.	2	0	0	2
20	Лабораторное занятие 10	0	0	2	2
21	Лекционное занятие 11.	2	0	0	2
22	Лабораторное занятие 11	0	0	2	2
23	Лекционное занятие 12.	2	0	0	2
24	Лабораторное занятие 12	0	0	2	2
25	Лекционное занятие 13.	2	0	0	2
26	Лабораторное занятие 13	0	0	2	2
27	Лекционное занятие 14.	2	0	0	2
28	Лабораторное занятие 14	0	0	2	2
29	Лекционное занятие 15.	2	0	0	2
30	Лабораторное занятие 15	0	0	2	2
31	Лекционное занятие 16.	2	0	0	2
32	Лабораторное занятие 16	0	0	2	2
33	Консультация перед зачетом	0	0	0	0

34	Зачет по дисциплине	0	0	0	0
	Итого часов	32	0	32	64

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 диф. зачета – 9 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 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: 15.05.2022).

2. 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: 15.05.2022).

3. 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: 15.05.2022).

5.2 Электронные образовательные 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/

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека https://rusneb.ru/

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

MS Office, платформа для электронного обучения Microsoft Teams, ОС MS Windows, ОС FreeBSD.

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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора Института
математики и компьютерных наук
М.Н. Перевалова
РАЗРАБОТЧИК(И)
Зулькарнеев И. Р.

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность компьютерных систем и сетей» (связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):ОПК-5*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

<u>Организационное и правовое обеспечение информационной безопасности</u>

В результате освоения дисциплины "Организационное и правовое обеспечение информационной безопасности" обучающийся должен

Знать:

- содержание основных понятий по правовому обеспечению информационной безопасности;
- правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности;
- понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации;
- правила лицензирования и сертификации в области защиты информации
- теоретические основы функционирования систем организационной защиты информации, ее современные проблемы и терминологию;
- основные направления и методы организационной защиты информации в организациях с различными формами собственности
- основные положения международных стандартов в области информационной безопасности

Уметь:

- отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
- применять действующую законодательную базу в области информационной безопасности;
- разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;
- анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития;

Владеть:

- умением работы с нормативно-правовыми актами;
- умением разработки нормативно-методических материалов по регламентации системы организационной защиты информации;
- навыками применения различных способов методов защиты информации по каналам утечки и от несанкционированного доступа к ней;
- навыками проектирования систем защиты информации

В процессе освоения дисциплины формируются следующие компетенции:

- способность использовать нормативные правовые акты в своей профессиональной деятельности
- способность участвовать в разработке проектной и технической документации
- способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы
- разрабатывать проекты нормативных, правовых и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			5
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося		80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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 5 семестре	32	32	0	64
	Организационное и правовое обеспечение информационной безопасности	32	32	0	64
1	Лекция 1	2	0	0	2
2	Практика 1	0	2	0	2
3	Лекция 2	2	0	0	2
4	Практика 2	0	2	0	2
5	Лекция 3	2	0	0	2
6	Практика 3	0	2	0	2
7	Лекция 4	2	0	0	2
8	Практика 4	0	2	0	2
9	Лекция 5	2	0	0	2
10	Практика 5	0	2	0	2
11	Лекция 6	2	0	0	2
12	Практика 6	0	2	0	2
13	Лекция 7	2	0	0	2
14	Практика 7	0	2	0	2
15	Лекция 8	2	0	0	2
16	Практика 8	0	2	0	2
17	Лекция 9	2	0	0	2
18	Практика 9	0	2	0	2
19	Лекция 10	2	0	0	2
20	Практика 10	0	2	0	2
21	Лекция 11	2	0	0	2
22	Практика 11	0	2	0	2
23	Лекция 12	2	0	0	2
24	Практика 12	0	2	0	2
25	Лекция 13	2	0	0	2
26	Практика 12	0	2	0	2
27	Лекция 14	2	0	0	2
28	Практика 14	0	2	0	2
29	Лекция 15	2	0	0	2
30	Практика 15	0	2	0	2

31	Лекция 16	2	0	0	2
32	Практика 16	0	2	0	2
33	Консультация перед экзаменом	0	0	0	0
34	Зачет с оценкой	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 (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.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Козьминых, С. И. Организационно-правовое обеспечение информационной безопасности : учебное пособие / С. И. Козьминых. - Тбилиси : Справедливая Грузия, 2022. - 309 с. - ISBN 978-9941-9663-2-3. - Текст : электронный. - URL: https://znanium.com/catalog/document?pid=1359091 (дата обращения: 10.05.2022)
2. 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: 10.05.2022)
3. 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: 10.05.2022).

5.2 Электронные образовательные ресурсы:

1. https://fstec.ru/ru/
2. http://fsb.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.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
заместитель директора
Института математики и
компьютерных наук
Перевалова М. Н.
РАЗРАБОТЧИК(И)
Ханбеков Ш. И.

Основы построения защищенных баз данных

Рабочая программа
для обучающихся по специальности 10.05.01 Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
Уровень высшего образования: специалитет
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ОПК-14

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Основы построения защищенных баз данных

Перечень планируемых результатов обучения по дисциплине:

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;
- нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- основные средства и способы обеспечения информационной безопасности, предоставляемые системами управления базами данных; - принципы построения систем защиты информации;

уметь:

- анализировать и оценивать угрозы информационной безопасности объекта;
- применять действующую законодательную базу в области обеспечения безопасности систем баз данных;
- применять отечественные и зарубежные стандарты для проектирования, разработки и оценивания защищенности компьютерной системы;
- формализовать поставленную задачу по обеспечению защиты БД;
- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- использовать средства защиты, предоставляемые системами управления базами данных;
- проводить обоснование и выбор рационального решения по защите систем управления баз данных с учетом заданных требований;

владеть:

- методиками использования средств защиты, предоставляемых системами управления базами данных;
- профессиональной терминологией в области информационной безопасности;
- практическими навыками работы с научно-технической документацией;
- навыками разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; - навыками разработки модели угроз и модели нарушителя безопасности компьютерных систем;
- навыками разработки частных политик безопасности, в том числе политик управления доступом и информационными потоками;
- методами анализа безопасности информационных систем на базе промышленных СУБД;
- навыками формирования требований по защите информации.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			7
Общая трудоемкость	**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 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 7 семестре	32	0	32	64
	Основы построения защищенных баз данных	32	0	32	64
1	Введение. Информационные системы. СУБД.	4	0	0	4
2	Ограничения целостности базы данных	0	0	2	2
3	Нормализация баз данных. 3НФ	0	0	2	2
4	Целостность БД и способы ее обеспечения. Первичные ключи. Индексирование в базах данных. Оптимизация запросов	4	0	0	4
5	Нормализация баз данных. 5НФ	0	0	2	2
6	Временные таблицы. Функции. процедуры	0	0	2	2
7	Первичные ключи. Индексирование в базах данных. Оптимизация запросов	4	0	0	4
8	Виды первичных ключей. Индексы. Оптимизация запросов.	0	0	2	2
9	Транзакции. Уровни изоляции транзакций	0	0	2	2
10	Транзакции и блокировки. Средства идентификации и аутентификации	4	0	0	4
11	Транзакции. Уровни изоляции транзакций	0	0	2	2
12	Аутентификация на уровне ОС и на уровне СУБД	0	0	2	2
13	Средства управления доступом. Шифрование в СУБД	4	0	0	4
14	Шифрование	0	0	2	2
15	"Управление доступом к базе данных	0	0	2	2
16	Критерии защищенности БД. Безопасность БД, угрозы, защита	4	0	0	4
17	Триггеры безопасности. Журналирование в СУБД	0	0	2	2

18	Резервное копирование и восстанволение. Модели восстановления	0	0	2	2
19	Модели безопасности в СУБД. Классификация угроз конфиденциальности СУБД	4	0	0	4
20	Журнал транзакций	0	0	2	2
21	Секционирование. Файловые группы базы данных	0	0	2	2
22	Аудит и подотчетность. Обзор. Другие программно-технические способы защиты информации	4	0	0	4
23	Распределенные базы данных	0	0	2	2
24	Группы высокой доступности	0	0	2	2
25	Консультация	0	0	0	0
26	Консультация	0	0	0	0
27	Экзамен	0	0	0	0
	Итого (ак.часов)	32	0	32	64

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 контрольной работы.

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. 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: 12.05.2022). – Режим доступа: по подписке.

2. 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: 12.05.2022). – Режим доступа: по подписке.

3. 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: 12.05.2022). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:

- вузовские электронно-библиотечные системы учебной литературы;
- вузовские электронно-библиотечные системы учебной литературы;
- база научно-технической информации ВИНИТИ РАН;
- доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, mathnet.ru;

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека. URL: https://rusneb.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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора Института
математики и компьютерных наук
М.Н. Перевалова
РАЗРАБОТЧИК
Шабалин А. М.

Основы построения защищенных компьютерных сетей
Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01 «Компьютерная безопасность»
Профиль «Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)»
форма обучения очная
Специалитет

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-10*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Основы построения защищенных компьютерных сетей

В результате освоения дисциплины студент должен

Знать:

- 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.

Уметь:

- 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.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			6
Общая трудоемкость	**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 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 6 семестре	32	0	32	64
	Основы построения защищенных компьютерных сетей	32	0	32	64
1	Лекция 1. Основы проектирования и работы безопасных коммутируемых сетей	2	0	0	2
2	Лабораторная работа 1. CAM и TCAM-таблицы. Варианты ускорения коммутации (route caching, topology-based switching)	0	0	2	2
3	Лекция 2. Типы коммутаторов.	2	0	0	2
4	Лабораторная работа 2. Безопасность коммутируемой среды в сети предприятия	0	0	2	2
5	Лекция 3. Работа с VLAN. Транки.	2	0	0	2
6	Лабораторная работа 3. Сегментирование сетей. Private VLAN, типы и настройка	0	0	2	2
7	Лекция 4. Предотвращение сетевых атак на виртуальные локальные сети	2	0	0	2
8	Лабораторная работа 4. Безопасность виртуальных локальных сетей	0	0	2	2
9	Лекция 5. Предотвращение сетевых атак на протоколы семейства Spanning Tree	2	0	0	2
10	Лабораторная работа 5. Безопасность протоколов семейства Spanning Tree	0	0	2	2
11	Лекция 6. Проектирование и настройка маршрутизации между VLAN.	2	0	0	2
12	Лабораторная работа 6. Включение протоколов динамической маршрутизации и обеспечение их безопасности	0	0	2	2
13	Консультация1	0	0	0	0

14	Лекция 7. Безопасная маршрутизация между сегментами внутри кампусной сети	2	0	0	2
15	Лабораторная работа 7. Безопасная маршрутизация средствами Multilayer Switch	0	0	2	2
16	Лекция 8. Предотвращение сетевых атак на беспроводные сети	2	0	0	2
17	Лабораторная работа 8. Безопасность беспроводных клиентов в сети предприятия	0	0	2	2
18	Лекция 9. Задачи протоколов семейства FHRP	2	0	0	2
19	Лабораторная работа 9. Использование FHRP-протоколов в сетях с IPv6	0	0	2	2
20	Лекция 10. Предотвращение сетевых атак на протоколы FHRP	2	0	0	2
21	Лабораторная работа 10. Безопасность протоколов первого хопа	0	0	2	2
22	Лекция 11. Основные вопросы безопасности коммутаторов access-уровня	2	0	0	2
23	Лабораторная работа 11. Защита от спуфинга	0	0	2	2
24	Консультация 2	0	0	0	0
25	Лекция 12. Безопасность коммутируемых сетей на уровне доступа (access)	2	0	0	2
26	Лабораторная работа 12. Предотвращение атак на уровне доступа в сети предприятия	0	0	2	2
27	Лекция 13. Централизованные службы по аутентификации, авторизации и учету RADIUS и TACACS+	2	0	0	2
28	Лабораторная работа 13. Работа с удалённым RADIUS-сервером. Настройка AAA	0	0	2	2
29	Лекция 14. Безопасность коммутируемых сетей на уровне распределения (distribution)	2	0	0	2
30	Лабораторная работа 14. Механизм защиты Storm Control, настройка и отслеживание срабатывания.	0	0	2	2
31	Лекция 15. Задачи и режимы работы протокола NTPv4. Протокол SNMPv3	2	0	0	2
32	Лабораторная работа 15. Настройка Port Mirroring (SPAN, RSPAN). Безопасность NTP	0	0	2	2
33	Лекция 16. Технологии отказоустойчивости, высокой доступности и мониторинга безопасности компьютерных сетей	2	0	0	2

34	Лабораторная работа 16. Сервисы и службы мониторинга безопасности компьютерных сетей	0	0	2	2
35	Консультация 3	0	0	0	0
36	Экзамен по дисциплине	0	0	0	0
	Итого (ак.часов)	32	0	32	64

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 экзамена.

– 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. 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.
2. 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.
3. 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.
4. 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.

5.2 Электронные образовательные ресурсы:

– MITRE ATT&CK. https://attack.mitre.org/
– Банк данных угроз безопасности информации. https://bdu.fstec.ru/vul

6. 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/

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

- MS Windows 10
- MS Office,
- Oracle Virtual Box
- GNS3
- платформа для электронного обучения Microsoft Teams.

8. Технические средства и материально-техническое обеспечение дисциплины

Мультимедийная учебная аудитория для проведения занятий лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

Компьютерный класс с выходом в интернет.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора Института
математики и компьютерных наук
М.Н. Перевалова
РАЗРАБОТЧИК(И)
Зулькарнеев И. Р.

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность компьютерных систем и сетей» (связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):ОПК-13*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Организационное и правовое обеспечение информационной безопасности

В результате освоения дисциплины обучающийся должен

Знать:

- методы защиты компьютерной информации;
- классификацию и общую характеристику программно-аппаратных средств защиты информации;
- основные принципы администрирования защищенных компьютерных систем;
- особенности реализации методов защиты информации программно-аппаратными средствами;

Уметь:

- выполнять функции администратора безопасности защищенных компьютерных систем;
- выполнять настройку защитных механизмов программно-аппаратных средств;
- настраивать политику безопасности средствами программно-аппаратных комплексов защиты информации;
- применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных систем;
- выполнять защиту рабочих мест с использованием программно-аппаратных средств защиты информации;

Владеть:

- средствами администрирования программно-аппаратных комплексов защиты информации от несанкционированного доступа;
- средствами администрирования комплексов криптографической защиты информации;
- средствами контроля и анализа защищенности

В процессе освоения дисциплины формируются следующие компетенции:

- 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
- 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
- способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций

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.**	8	4	4
	час	288	144	144
Из них:				
Часы аудиторной работы (всего):		124	64	60
Лекции		62	32	30
Практические занятия		62	32	30
Лабораторные / практические занятия по подгруппам		0	0	0
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		164	80	84
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный зачет	Дифференцированный 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	32	32	0	64
	Программно-аппаратные средства защиты информации	32	32	0	64
1	Введение. Определение СрЗИ	2	0	0	2
2	Классификация СрЗИ	2	0	0	2
3	Оценка функционала и принципов работы СрЗИ	0	2	0	2
4	Виды СрЗИ	2	0	0	2
5	Оценка функционала и принципов работы СрЗИ	0	2	0	2
6	Виды СрЗИ	2	0	0	2
7	Оценка функционала и принципов работы СрЗИ	0	2	0	2
8	Виды СрЗИ	2	0	0	2
9	Система сертификации СрЗИ в РФ	2	0	0	2
10	Профили защиты, ЗБ и ТУ	2	0	0	2
11	Подготовка материалов к сертификации	0	2	0	2
12	Классификация СВТ, НДВ, СДЗ,СКСМНИ	2	0	0	2
13	Подготовка материалов к сертификации	0	2	0	2
14	Классификация МЭ, СОВ, АВЗ, ОС	2	0	0	2
15	Подготовка материалов к сертификации	0	2	0	2
16	Обеспечение комплексной безопасности конечных точек	2	0	0	2
17	СДЗ Соболь	2	0	0	2
18	СДЗ Соболь	2	0	0	2
19	Подготовка к установке ПАК Соболь	0	2	0	2
20	Установка и настройка ПАК Соболь	0	2	0	2
21	Secret Net Studio	2	0	0	2
22	Secret Net Studio	0	2	0	2
23	Secret Net Studio	0	2	0	2

24	Secret Net Studio	2	0	0	2
25	Secret Net Studio	0	2	0	2
26	Secret Net Studio	0	2	0	2
27	Secret Net Studio	2	0	0	2
28	Secret Net Studio	0	2	0	2
29	Secret Net Studio	2	0	0	2
30	Secret Net Studio	0	2	0	2
31	Secret Net Studio	0	2	0	2
32	Secret Net Studio	0	2	0	2
33	Консультация	0	0	0	0
34	Зачет с оценкой	0	0	0	0
	Итого за 7 семестр (ак.часов)	32	32	0	64
	Часов в 8 семестре	30	30	0	60
	Программно-аппаратные средства защиты информации	30	30	0	60
1	Установка и администрирование ViPNet	2	0	0	2
2	Установка и администрирование ViPNet	0	2	0	2
3	Установка и администрирование ViPNet	2	0	0	2
4	Установка и администрирование ViPNet	0	2	0	2
5	Установка и администрирование ViPNet	2	0	0	2
6	Установка и администрирование ViPNet	0	2	0	2
7	Установка и администрирование ViPNet	2	0	0	2
8	Установка и администрирование ViPNet	0	2	0	2
9	Установка и администрирование ViPNet	2	0	0	2
10	Установка и администрирование ViPNet	0	2	0	2
11	Установка и администрирование ViPNet	2	0	0	2
12	Установка и администрирование ViPNet	0	2	0	2
13	Установка и администрирование АПКШ "Континент"	2	0	0	2
14	Установка и администрирование АПКШ "Континент"	0	2	0	2
15	Установка и администрирование АПКШ "Континент"	2	0	0	2
16	Установка и администрирование АПКШ "Континент"	0	2	0	2
17	Установка и администрирование xSpider	2	0	0	2
18	Установка и администрирование xSpider	0	2	0	2

19	Установка и администрирование PT Application Firewall	2	0	0	2
20	Установка и администрирование PT Application Firewall	0	2	0	2
21	Установка и администрирование PT Application Firewall	2	0	0	2
22	Установка и администрирование PT Application Firewall	0	2	0	2
23	Установка и администрирование PT Application Firewall	2	0	0	2
24	Установка и администрирование PT Application Firewall	0	2	0	2
25	Установка и администрирование PT Application Firewall	2	0	0	2
26	Установка и администрирование PT Application Firewall	0	2	0	2
27	Установка и администрирование PT MaxPatrol	2	0	0	2
28	Установка и администрирование PT MaxPatrol	0	2	0	2
29	Установка и администрирование PT MaxPatrol	2	0	0	2
30	Установка и администрирование PT MaxPatrol	0	2	0	2
31	Консультация	0	0	0	0
32	Консультация	0	0	0	0
33	Зачет с оценкой	0	0	0	0
	Итого за 8 семестр (ак.часов)	30	30	0	60
	Итого за оба семестра (ак.часов)	62	62	0	124

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 диф. зачета в 7 и 8 семестрах.

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. 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: 10.05.2020). – Режим доступа: по подписке
2. 1Хорев, 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: 10.05.2020). – Режим доступа: по подписке.
3. 2Аппаратно-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: 10.05.2020). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:

1. https://fstec.ru/
2. 2сайты компаний-производителей средств защиты информацииhttps://fstec.ru/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

- программное обеспечение виртуализации: VirtualBox или аналог
- операционная система Windows 7 или более поздние версии
- установленное ПО: MS Office
- платформа для электронного обучения Microsoft Teams

Специализированное лицензионное программное обеспечение из п.8.

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 семинарского типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, проектор, не менее 13 персональных компьютеров

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,

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
Перевалова М.Н.
РАЗРАБОТЧИК
Оленников А. А.

РАЗРАБОТКА И ЗАЩИТА WEB-ПРИЛОЖЕНИЙ

Рабочая программа для
обучающихся по специальности
10.05.01. Компьютерная
безопасность
специализация «Безопасность компьютерных систем и сетей (связь,
информационные и коммуникационные технологии)»
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-7*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Разработка и защита web-приложений 1

В результате освоения ОП выпускник должен обладать следующими компетенциями:

- Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ (ОПК-7).

В результате освоения дисциплины студент должен

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.

Разработка и защита web-приложений 2

В результате освоения ОП выпускник должен обладать следующими компетенциями:

 Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ (ОПК-7).

В результате освоения дисциплины студент должен

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.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**	
			5	6
Общая трудоемкость	**зач. ед.**	8	4	4
	час	288	144	144
Из них:				
Часы аудиторной работы (всего):		128	64	64
Лекции		64	32	32
Практические занятия		0	0	0
Лабораторные / практические занятия по подгруппам		64	32	32
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		160	80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный зачет	Дифференцированный 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 / практическио подгруппам	
1	2	3	4	5	6
	Часов в 5 семестре	32	0	32	64
	Разработка и защита web-приложений 1	32	0	32	64
1	Введение	2	0	0	2
2	Лабораторная работа	0	0	2	2
3	Введение	2	0	0	2
4	Лабораторная работа	0	0	2	2
5	Протокол HTML	2	0	0	2
6	Лабораторная работа	0	0	2	2
7	Протокол HTML	2	0	0	2
8	Лабораторная работа	0	0	2	2
9	Протокол HTML	2	0	0	2
10	Лабораторная работа	0	0	2	2
11	Протокол HTML	2	0	0	2
12	Лабораторная работа	0	0	2	2
13	Веб клиент	2	0	0	2
14	Лабораторная работа	0	0	2	2
15	Веб клиент	2	0	0	2
16	Лабораторная работа	0	0	2	2
17	Веб клиент	2	0	0	2
18	Лабораторная работа	0	0	2	2
19	Веб клиент	2	0	0	2
20	Лабораторная работа	0	0	2	2
21	Веб сервер	2	0	0	2
22	Лабораторная работа	0	0	2	2
23	Веб сервер	2	0	0	2
24	Лабораторная работа	0	0	2	2
25	Веб сервер	2	0	0	2
26	Лабораторная работа	0	0	2	2
27	Веб сервер	2	0	0	2

28	Лабораторная работа	0	0	2	2
29	Веб сервер	2	0	0	2
30	Лабораторная работа	0	0	2	2
31	Веб сервер	2	0	0	2
32	Лабораторная работа	0	0	2	2
33	Консультация	0	0	0	0
34	Дифференцированный зачет	0	0	0	0
	Часов в 6 семестре	32	0	32	64
	Разработка и защита web-приложений 2	32	0	32	64
1	Веб сервер	2	0	0	2
2	Лабораторная работа 1	0	0	2	2
3	Веб сервер	2	0	0	2
4	Лабораторная работа 2	0	0	2	2
5	Веб сервер	2	0	0	2
6	Лабораторная работа 3	0	0	2	2
7	Веб сервер	2	0	0	2
8	Лабораторная работа 4	0	0	2	2
9	Веб сервер	2	0	0	2
10	Лабораторная работа 5	0	0	2	2
11	Веб сервер	2	0	0	2
12	Лабораторная работа 6	0	0	2	2
13	Веб сервер	2	0	0	2
14	Лабораторная работа 7	0	0	2	2
15	Веб сервер	2	0	0	2
16	Лабораторная работа 8	0	0	2	2
17	Веб сервер	2	0	0	2
18	Лабораторная работа 9	0	0	2	2
19	Веб сервер	2	0	0	2
20	Лабораторная работа 10	0	0	2	2
21	Веб сервер	2	0	0	2
22	Лабораторная работа 11	0	0	2	2
23	Веб сервер	2	0	0	2
24	Лабораторная работа 12	0	0	2	2
25	Веб сервер	2	0	0	2
26	Лабораторная работа 13	0	0	2	2
27	Веб сервер	2	0	0	2
28	Лабораторная работа 14	0	0	2	2
29	Веб сервер	2	0	0	2
30	Лабораторная работа 15	0	0	2	2
31	Веб сервер	2	0	0	2
32	Лабораторная работа 16	0	0	2	2
33	Консультация	0	0	0	0
34	Дифференцированный зачет	0	0	0	0
	Итого (ак.часов)	64	0	64	128

4. Система оценивания.

В 5 и 6 семестрах предусмотрен дифференцированный зачет. Зачет с оценкой является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и 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 зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных 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 90% лабораторных 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 лабораторные 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 оценку, полученную в рамках модульнорейтинговой системы, имеет право на сдачу зачета или выполнение дополнительного задания на усмотрение преподавателя.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 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: 20.09.2022). – Режим доступа: для авториз. пользователей.
2. 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: 20.09.2022). – Режим доступа: для авториз. пользователей.

3. 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: 20.09.2022). – Режим доступа: для авториз. пользователей.

5.2 Электронные образовательные ресурсы:

1. Научная электронная библиотека. URL: http://elibrary.ru/.
2. Электронные ресурсы ИБЦ ТюмГУ. URL: https://bmk.utmn.ru/ru/.

6. 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

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

- MS Office, платформа для электронного обучения Microsoft Teams.
- 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. □ Программное обеспечение виртуализации: VirtualBox (бесплатная лицензия доступна: https://www.virtualbox.org/wiki/Downloads).

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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.
- Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора Института
математики и компьютерных наук
М.Н. Перевалова
РАЗРАБОТЧИК
Шабалин А. М.

Сети и системы передачи информации
Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01 «Компьютерная безопасность»
Профиль «Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)»
форма обучения очная
Специалитет

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК 4.1*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Сети и системы передачи информации

В результате изучения дисциплины студент должен:

Знать:

– Принципы связи и обмен данными в локальной проводной сети;

– Уровни доступа и распределения в сети Ethernet;

– Структуру сети Интернет, принципы обмена данными между узлами в Интернет;

– Схему подключения к Интернету через поставщика услуг;

– Сетевые устройства;

– Виды, характеристики и маркировку сетевых кабелей и контактов;

– Принципы сетевой адресации, формат IP-адреса и маски подсети, типы IP-адресов и методы их получения, протокол DHCP;

– Многоуровневую модель межсетевого взаимодействия OSI и сетевые протоколы;

– Беспроводные технологии для локальных сетей;

–Основные сетевые службы, архитектуру клиент-сервер, IP-сервисы и принципы их работы, сервис электронной почты, сервис доменных имен DNS;

– Архитектуру и возможности систем Cisco IOS / Huawei VRP;

– Основные протоколы маршрутизации;

– Структуру IP-адресации в ЛВС;

–Методы трансляции адресов NAT и PAT;

– Базовые настройки маршрутизаторов;

– Базовые настройки коммутаторов;

– Механизмы резервного копирования и аварийного восстановления в сети.

Уметь:

– Проектировать и устанавливать домашнюю сеть или сеть малого предприятия, а также подключать ее к сети Интернет;

– Выполнять проверку и устранять неполадки сети и подключения к сети Интернет;

– Обеспечивать общий доступ нескольких компьютеров к сетевым ресурсам (файлам, принтерам и др.);

– Выявлять и устранять угрозы безопасности локальной компьютерной сети;

– Настраивать и проверять базовые Интернет-приложения;

– Настраивать базовые IP-сервисы при помощи графического интерфейса ОС;

– Устанавливать и настраивать устройства для подключения к сети Интернет и серверам, выполнять поиск и устранение неполадок;

–Проектировать базовую проводную инфраструктуру для поддержки сетевого трафика;

– Обеспечивать подключение к сети WAN на базе сервисов телекоммуникационных компаний;

– Выполнять адекватные процедуры восстановления при авариях и осуществлять резервирование сервера;

– Контролировать производительность сети и выявлять сбои;

–Выявлять и устранять неполадки с использованием структурированной многоуровневой процедуры.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**	
			4	5
Общая трудоемкость	**зач. ед.**	8	4	4
	час	288	144	144
Из них:				
Часы аудиторной работы (всего):		128	64	64
Лекции		64	32	32
Практические занятия		0	0	0
Лабораторные / практические занятия по подгруппам		64	32	32
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		160	80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный зачет	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 4 семестре	32	0	32	64
	Сети и системы передачи информации	32	0	32	64
1	Лекция 1. Аппаратное обеспечение для персонального компьютера	2	0	0	2
2	Лабораторная работа 1. Базовые операции по установке и настройке устройств:	0	0	2	2
3	Лекция 2. Компоненты компьютера и периферийные устройства.	2	0	0	2

4	Лабораторная работа 2. Планирование структуры локальной сети и подключение устройств.	0	0	2	2
5	Лекция 3. Сетевые устройства в NOC. Кабели и контакты.	2	0	0	2
6	Лабораторная работа 3. Прокладка кабелей "витая пара".	0	0	2	2
7	Лекция 4. Сетевая адресация. Сетевые службы.	2	0	0	2
8	Лабораторная работа 4. Создание и настройка одноранговой сети	0	0	2	2
9	Лекция 5. Типы IP-адресов. Получение IP-адресов и управление ими.	2	0	0	2
10	Лабораторная работа 5. Определение IP-адреса компьютера. Изучение сетевого взаимодействия на базе IP-адресов	0	0	2	2
11	Лекция 6. Многоуровневая модель и протоколы.	2	0	0	2
12	Лабораторная работа 6. Прикладные протоколы и сервисы.	0	0	2	2
13	Лекция 7. Беспроводные локальные сети.	2	0	0	2
14	Лабораторная работа 7. Настройка интегрированной точки доступа и беспроводного клиента.	0	0	2	2
15	Лекция 8. Обеспечение безопасности беспроводной локальной сети.	2	0	0	2
16	Лабораторная работа 8. Сетевые угрозы. Методы атак.	0	0	2	2
17	Лекция 9. Основы сетевой безопасности.	2	0	0	2
18	Лабораторная работа 9. Использование межсетевых экранов.	0	0	2	2
19	Лекция 10. Устранение проблем с сетями.	2	0	0	2
20	Лабораторная работа 10. Устранение неполадок и справочная служба.	0	0	2	2
21	Лекция 11. Интернет и возможности его использования.	2	0	0	2
22	Лабораторная работа 11. Создание компьютерной сети с помощью маршутизатора	0	0	2	2
23	Консультация 1	0	0	0	0
24	Лекция 12. Поставщики услуг Интернета (ISP).	2	0	0	2
25	Лабораторная работа 12. Предоставление общего доступа к сетевым ресурсам	0	0	2	2
26	Лекция 13. Связь с поставщиком интернет-услуг.	2	0	0	2

27	Лабораторная работа 13. Основные команды для проверки подключения к Интернету.	0	0	2	2
28	Лекция 14. Служба технической поддержки.	2	0	0	2
29	Лабораторная работа 14. Подключение компьютера к сети с помощью кабелей	0	0	2	2
30	Лекция 15. Модель OSI.	2	0	0	2
31	Лабораторная работа 15. Создание прямых и перекрещенных кабелей «неэкранированная витая пара»	0	0	2	2
32	Лекция 16. Устранение неполадок на уровне поставщика интернет-услуг.	2	0	0	2
33	Лабораторная работа 16. Тестирование кабелей «неэкранированная витая пара»	0	0	2	2
34	Консультация 2	0	0	0	0
35	Зачет по дисциплине	0	0	0	0
	Часов в 5 семестре	32	0	32	64
	Сети и системы передачи информации	32	0	32	64
1	Лекция 1. Планирование обновления сети	2	0	0	2
2	Лабораторная работа 1. Изучение принципов работы DNS	0	0	2	2
3	Лекция 2. Общие проблемы и планирование обновления сети. Приобретение и обслуживание оборудования.	2	0	0	2
4	Лабораторная работа 2. Изучение протокола FTP	0	0	2	2
5	Лекция 3. Планирование структуры адресации.	2	0	0	2
6	Лабораторная работа 3. Поиск и устранение проблем в компьютерных сетях	0	0	2	2
7	Лекция 4. IP-адресация в ЛВС.	2	0	0	2
8	Лабораторная работа 4. Настройка точки беспроводного доступа	0	0	2	2
9	Лекция 5. NAT и PAT.	2	0	0	2
10	Лабораторная работа 5. Настройка беспроводной сетевой карты	0	0	2	2
11	Лекция 6. Настройка сетевых устройств	2	0	0	2
12	Лабораторная работа 6. Настройка безопасности в беспроводной сети	0	0	2	2
13	Консультация	0	0	0	0
14	Лекция 7. Маршрутизация	2	0	0	2
15	Лабораторная работа 7. Настройка безопасности компьютерной сети	0	0	2	2

16	Лекция 8. Применение протоколов маршрутизации.	2	0	0	2
17	Лабораторная работа 8. Первичная настройка маршрутизатора	0	0	2	2
18	Лекция 9. Протоколы внешней маршрутизации.	2	0	0	2
19	Лабораторная работа 9. Настройка маршрутизатора с использованием интерфейса командной строки IOS	0	0	2	2
20	Лекция 10. Службы поставщиков услуг Интернета.	2	0	0	2
21	Лабораторная работа 10. Настройка коммутатора	0	0	2	2
22	Лекция 11. Введение в сервисы поставщиков услуг Интернета.	2	0	0	2
23	Лабораторная работа 11. Планирование модернизации WAN	0	0	2	2
24	Консультация 2	0	0	0	0
25	Лекция 12. Инструментальные средства безопасности.	2	0	0	2
26	Лабораторная работа 12. Настройка удаленного маршрутизатора с помощью протокола SSH	0	0	2	2
27	Лекция 13. Протоколы, используемые для предоставления сервисов провайдерами. Служба доменных имен.	2	0	0	2
28	Лабораторная работа 13. Работа с IP маршрутизацией и протоколами маршрутизации	0	0	2	2
29	Лекция 14. Поиск и устранение неисправностей в сети.	2	0	0	2
30	Лабораторная работа 14. Работа с системой доменных имен DNS	0	0	2	2
31	Лекция 15. Устранение неполадок.	2	0	0	2
32	Лабораторная работа 15. Организация системы безопасности в сети:	0	0	2	2
33	Лекция 16. Методики и средства поиска и устранения неполадок.	2	0	0	2
34	Лабораторная работа 16. Обслуживание компьютерной сети	0	0	2	2
35	Консультация 3	0	0	0	0
36	Экзамен по дисциплине	0	0	0	0
	Итого (ак.часов)	64	0	64	128

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 диф. зачета в 4 семестре, в форме экзамена в 5 семестре.

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. 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.
2. 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.
3. 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.
4. 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.

5.2 Электронные образовательные ресурсы:

– MITRE ATT&CK. https://attack.mitre.org/
– Банк данных угроз безопасности информации. https://bdu.fstec.ru/vul

6. 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/

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

- MS Windows 10
- MS Office,

- Oracle Virtual Box
- GNS3
- платформа для электронного обучения Microsoft Teams.

8. Технические средства и материально-техническое обеспечение дисциплины

Мультимедийная учебная аудитория для проведения занятий лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

Компьютерный класс с выходом в интернет.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
Перевалова М.Н.
РАЗРАБОТЧИК
Оленников А. А.

СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

Рабочая программа для
обучающихся по специальности
10.05.01. Компьютерная
безопасность
специализация «Безопасность компьютерных систем и сетей (связь,
информационные и коммуникационные технологии)»
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-2.*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Системы видеонаблюдения

В результате освоения ОП выпускник должен обладать следующими компетенциями:

- Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности (ОПК-2).

В результате освоения ОП выпускник должен:

знать:

- основные понятия систем видеонаблюдения;
- нормативно-техническую документацию;
- основные понятия аппаратных средств систем видеонаблюдения;
- основы базовых технологий систем видеонаблюдения;
- принцип работы устройств видеонаблюдения; **уметь:**

- формализовать поставленную задачу;
- осуществлять аппаратную реализации состава системы;
- проектировать сети систем видеонаблюдения;
- осуществлять настройку систем видеонаблюдения;
- проводить анализ и монитоинг сетей и узлов видеонаблюдения.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			9
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося		80	80

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

3. Содержание дисциплины

Таблица 2

№	Тематика учебных встреч	Виды аудиторной работы (в ак.час.)			Итого аудиторных ак.часов по теме
		Лекции	П	Лабораторные / практические занятия по подгруппам	
1	2	3	4	5	6
	Часов в 9 семестре	32	0	32	64
	Системы видеонаблюдения	32	0	32	64
1	Лекционное занятие 1	2	0	0	2
2	Лабораторное занятие 1	0	0	2	2
3	Лекционное занятие 2	2	0	0	2
4	Лабораторное занятие 2	0	0	2	2
5	Лекционное занятие 3	2	0	0	2
6	Лабораторное занятие 3	0	0	2	2
7	Лекционное занятие 4	2	0	0	2
8	Лабораторное занятие 2	0	0	2	2
9	Лекционное занятие 5	2	0	0	2
10	Лабораторное занятие 5	0	0	2	2
11	Лекционное занятие 6	2	0	0	2
12	Лабораторное занятие 6	0	0	2	2
13	Лекционное занятие 7	2	0	0	2
14	Лабораторное занятие 7	0	0	2	2
15	Лекционное занятие 8	2	0	0	2
16	Лабораторное занятие 8	0	0	2	2
17	Лекционное занятие 9	2	0	0	2
18	Лабораторное занятие 9	0	0	2	2
19	Лекционное занятие 10	2	0	0	2
20	Лабораторное занятие 10	0	0	2	2
21	Лекционное занятие 11	2	0	0	2
22	Лабораторное занятие 11	0	0	2	2
23	Лекционное занятие 12	2	0	0	2
24	Лабораторное занятие 12	0	0	2	2
25	Лекционное занятие 13	2	0	0	2

26	Лабораторное занятие 13	0	0	2	2
27	Лекционное занятие 14	2	0	0	2
28	Лабораторное занятие 14	0	0	2	2
29	Лекционное занятие 15	2	0	0	2
30	Лабораторное занятие 15	0	0	2	2
31	Лекционное занятие 16	2	0	0	2
32	Лабораторное занятие 16	0	0	2	2

33	Консультация перед зачетом	0	0	0	0
34	Дифференцированный зачет	0	0	0	0
	Итого (ак.часов)	32	0	32	64

4. Система оценивания.

В 9 семестре предусмотрен дифференцированный зачет. Зачет с оценкой является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и 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 зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных 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 90% лабораторных 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 лабораторные 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 оценку, полученную в рамках модульнорейтинговой системы, имеет право на сдачу зачета или выполнение дополнительного задания на усмотрение преподавателя.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1.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: 20.09.2022). – Режим доступа: по подписке.
2. Землянухин, П. А. Видео- и радиосигналы в системах передачи информации : учебное пособие / П.А. Землянухин ; Южный федеральный университет. - Ростовна-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: 20.09.2022). – Режим доступа: по подписке.

3. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРАМ, 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: 20.09.2022). – Режим доступа: по подписке.

5.2.Электронные образовательные ресурсы:

1. Научная электронная библиотека. URL: http://elibrary.ru/.
2. Электронные ресурсы ИБЦ ТюмГУ. URL: https://bmk.utmn.ru/ru/.

6. 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

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

- MS Office, платформа для электронного обучения Microsoft Teams.
- 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);
- Программное обеспечение виртуализации: VirtualBox (бесплатная лицензия доступна: https://www.virtualbox.org/wiki/Downloads).

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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.
- Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместителем директора
института Переваловой М.Н.
РАЗРАБОТЧИК(И)
Шабалин А. М.

Системы виртуализации

Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01. Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): (указываются только коды)*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения: ОПК-9.

Системы виртуализации

Знать:

принципы функционирования облачной инфраструктуры;

- состав и структуру технологий виртуализации;
- методы и средства создания виртуальных инфраструктур;
- методику проектирования, разработки и сопровождения виртуальных инфраструктур.

Уметь:

формулировать требования к виртуальной инфраструктуре;

- разрабатывать сценарии создания и генерации виртуальных инфраструктур;
- управлять состоянием инфраструктуры.

Владеть:

инструментами управления современными облачных сервисов и систем виртуализации;

- методологией внедрения систем виртуализации на предприятии;
- способами создания конфигураций виртуальной инфраструктуры;
- приемами мониторинга виртуальной системы, управления виртуальной системой.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			10
Общая трудоемкость	**зач. ед.**	4	4
	час	144	144
Из них:			
Часы аудиторной работы (всего):		60	60
Лекции		30	30
Практические занятия		30	30
Лабораторные / практические занятия по подгруппам		0	0
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		84	84
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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 10 семестре	30	30	0	60
	Системы виртуализации	30	30	0	60
1	Лекционное занятие 1	2	0	0	2
2	Практическое занятие 1	0	2	0	2
3	Лекционное занятие 2	2	0	0	2
4	Практическое занятие 2	0	2	0	2
5	Лекционное занятие 3	2	0	0	2
6	Практическое занятие 3	0	2	0	2
7	Лекционное занятие 4	2	0	0	2
8	Практическое занятие 4	0	2	0	2
9	Лекционное занятие 5	2	0	0	2
10	Практическое занятие 5	0	2	0	2
11	Консультация 1	0	0	0	0
12	Лекционное занятие 6	2	0	0	2
13	Практическое занятие 6	0	2	0	2
14	Лекционное занятие 7	2	0	0	2
15	Практическое занятие 7	0	2	0	2
16	Лекционное занятие 8	2	0	0	2
17	Практическое занятие 8	0	2	0	2
18	Лекционное занятие 9	2	0	0	2
19	Практическое занятие 9	0	2	0	2
20	Лекционное занятие 10	2	0	0	2
21	Практическое занятие 10	0	2	0	2
22	Консультация 1	0	0	0	0
23	Лекционное занятие 11	2	0	0	2
24	Практическое занятие 11	0	2	0	2
25	Лекционное занятие 12	2	0	0	2
26	Практическое занятие 12	0	2	0	2
27	Лекционное занятие 13	2	0	0	2
28	Практическое занятие 13	0	2	0	2
29	Лекционное занятие 14	2	0	0	2
30	Практическое занятие 14	0	2	0	2
31	Лекционное занятие 15	2	0	0	2
32	Практическое занятие 15	0	2	0	2

33	Консультация 1	0	0	0	0
34	Зачет с оценкой	0	0	0	0
	Итого (ак.часов)	30	30	0	60

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 диф. 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Савельев, А. О. Решения Microsoft для виртуализации ИТ-инфраструктуры предприятий : учебное пособие / А. О. Савельев. — 2-е изд. — Москва : ИНТУИТ, 2016. — 284 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100484 (дата обращения: 21.11.2022).
2. Ларина Т.Б. Виртуализация операционных систем : учебное пособие / Ларина Т.Б.. — Москва : Российский университет транспорта (МИИТ), 2020. — 65 с. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/115824.html (дата обращения: 22.11.2022).

5.2 Электронные образовательные 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.

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека https://rusneb.ru/

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

MS Office, платформа для электронного обучения Microsoft Teams, ОС MS Windows, ОС FreeBSD.

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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
заместитель директора
Института математики и
компьютерных наук
Перевалова М. Н.
РАЗРАБОТЧИК(И)
Ханбеков Ш. И.

Системы управления базами данных

Рабочая программа
для обучающихся по специальности 10.05.01 Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
Уровень высшего образования: специалитет
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ОПК-14

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Системы управления базами данных

В результате изучения курса студент должен:
знать

- типологию и методологию проектирования баз данных, уметь классифицировать информационные задачи, решаемые с использованием баз данных;
- особенности моделирования и проектирования реляционных баз данных;
- о целях и средствах разработки и администрирования баз данных;

уметь

- применять навыки разработки баз данных на практике;

иметь навыки

- владения системным подходом как методологической основой проектирования информационных систем, использующих базы данных;
- владения методикой составления запросов на языке SQL.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			5
Общая трудоемкость	**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 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 5 семестре	32	0	32	64
	Системы управления базами данных	32	0	32	64
1	Вводная лекция	4	0	0	4
2	SQL. Операторы DDL	0	0	2	2
3	SQL. Операторы DDL	0	0	2	2
4	Организация современной СУБД	4	0	0	4
5	SQL. Представления, процедуры, функции.	0	0	2	2
6	Реализация декларативной целостности в БД	0	0	2	2
7	Логические модели данных	4	0	0	4
8	Реализация процедурной целостности в БД	0	0	2	2
9	Язык запросов SQL: запросы модификации данных	0	0	2	2
10	Нормализация данных в реляционной модели	4	0	0	4
11	Нормализация	0	0	2	2
12	Нормализация	0	0	2	2
13	Язык запросов SQL: оконные функции, специальные конструкции	4	0	0	4
14	Оператор SELECT	0	0	2	2
15	SQL. Оконные функции и специальные операторы	0	0	2	2
16	Древововидные структуры. Реализация в реляционной модели. Рекурсивые запросы SQL.	4	0	0	4
17	SQL. Рекурсивные запросы для древовидных структур. Сравнение быстродействия.	0	0	2	2
18	Разработка базы данных с использованием СУБД HBase	0	0	2	2
19	Оптимизация выполнения запросов	4	0	0	4
20	Оптимизация запросов	0	0	2	2

21	Разработка картографическое приложения в PostGIS	0	0	2	2
22	Сравнение производительности СУБД	4	0	0	4
23	Тесты на скорость вставки и чтения для двух СУБД (на выбор)	0	0	2	2
24	Тесты на скорость вставки и чтения для двух СУБД (на выбор)	0	0	2	2
25	Консультация	0	0	0	0
26	Экзамен	0	0	0	0
	Итого (ак.часов)	32	0	32	64

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 контрольной работы.

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. Стасышин, В.М. Проектирование информационных систем и баз данных: учебное пособие / В.М. Стасышин. - Новосибирск : НГТУ, 2012. - 100 с. - ISBN 978-5-7782-2121-5; То же [Электронный ресурс]. - URL: http://znanium.com/catalog/product/548234. (дата обращения: 12.05.2022).

2. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учеб. пособие / В.Ф. Шаньгин. — М.: ИД «ФОРУМ» : ИНФРА-М, 2018. — 592 с.; [Электронный ресурс]. - URL: http://znanium.com/catalog/product/937502. (дата обращения: 12.05.2022).

3. Разработка и эксплуатация автоматизированных информационных систем : учеб. пособие / Л.Г. Гагарина. — М. : ИД «ФОРУМ» : ИНФРА-М, 2018.; [Электронный ресурс]. - URL: http://znanium.com/catalog/product/942717. (дата обращения: 12.05.2022).

5.2 Электронные образовательные ресурсы:

- вузовские электронно-библиотечные системы учебной литературы;
- вузовские электронно-библиотечные системы учебной литературы;
- база научно-технической информации ВИНИТИ РАН;
- доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, mathnet.ru;

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека. URL: https://rusneb.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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМКН
Перевалова М.Н.
РАЗРАБОТЧИК(И)
Ниссенбаум О.В.

Теоретико-числовые методы в криптографии

Рабочая программа
для обучающихся по специальности 10.05.01. Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
Уровень высшего образования: специалитет
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ОПК-10

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:
Теоретико-числовые методы в криптографии

знать:
- об основных задачах и понятиях криптографии;
- о теоретико-числовых основах двухключевой криптографии;
- основы дискретной алгебры и теории чисел;
- основные виды асимметричных криптографических алгоритмов;
- 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;
- корректно применять асимметричные криптографические алгоритмы;
- формализовать поставленную задачу;
- выполнить постановку задач криптоанализа и указать подходы к их решению;
- использовать основные математические методы, применяемые в синтезе и анализе типовых криптографических алгоритмов.

владеть:
- криптографической терминологией;
- навыками применения алгоритмов, основанных на теоретико-числовых принципах, к вопросам построения криптосистем и их анализу;
- навыками использования современной научно-технической литературы в области криптографической защиты
- навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			7
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося		80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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	32	32	0	64
	Теоретико-числовые методы в криптографии	32	32	0	64
1	Теория делимости	2	0	0	2
2	Основы теории делимости	0	2	0	2
3	Свойства целых чисел.	2	0	0	2
4	Основы теории делимости	0	2	0	2
5	Теоретико-числовые функции	2	0	0	2
6	Простые числа. Теоретико-числовые функции.	0	2	0	2
7	Теория сравнений	2	0	0	2
8	Теория сравнений	0	2	0	2
9	Обратный элемент и криптосистема RSA	2	0	0	2
10	Алгоритмы Евклида.	0	2	0	2
11	Сравнения с одним неизвестным	2	0	0	2
12	Сравнения первой степени и криптосистема	0	2	0	2
13	Теория квадратичных вычетов.	2	0	0	2
14	Системы сравнений 1-й степени и сравнения произвольной степени.	0	2	0	2
15	Решение квадратичных сравнений по простому модулю.	2	0	0	2
16	Символы Лежандра и Якоби. Квадратичные сравнения по простому модулю.	0	2	0	2
17	Решение квадратичных сравнений по составному модулю.	2	0	0	2
18	Решение квадратичных сравнений по составному модулю.	0	2	0	2
19	Квадратичные сравнения по модулю RSA.	2	0	0	2
20	Криптосистемы на основе теории квадратичных вычетов	0	2	0	2

21	Циклические мультипликативные группы и подгруппы вычетов.	2	0	0	2
22	Порядок элемента. Порождающий элемент.	0	2	0	2
23	Дискретный логарифм.	2	0	0	2
24	Доказуемо простые числа.	0	2	0	2
25	Доказуемо простые числа	2	0	0	2
26	Криптосистемы на основе дискретного логарифмирование.	0	2	0	2
27	Алгоритмы факторизации	2	0	0	2
28	Алгоритмы факторизации	0	2	0	2
29	Алгоритмы дискретного логарифмирования.	2	0	0	2
30	Алгоритмы факторизации и дискретного логарифмирования.	0	2	0	2
31	Алгоритмы дискретного логарифмирования.	2	0	0	2
32	Алгоритмы дискретного логарифмирования.	0	2	0	2
33	Консультация перед экзаменом.	0	0	0	0
34	Консультация	0	0	0	0
35	Теоретико-числовые методы в криптографии	0	0	0	0
	Итого (ак.часов)	32	32	0	64

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 дифференцированный зачет в устной форме.

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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

Основная литература:

1.Ильин, М. Е. Теоретико-числовые методы в криптографии. Ч.1 : учебное пособие / М. Е. Ильин, К. А. Ципоркова Теоретико-числовые методы в криптографии. Ч.1, 2027-05-23 Электрон. дан. (1 файл) Рязань: Рязанский государственный радиотехнический университет, 2020 112 с. Книга находится в премиум-версии IPR SMART. Гарантированный срок размещения в ЭБС до 23.05.2027 (автопролонгация) Текст электронный https://www.iprbookshop.ru/121800.html ISBN 2227-8397

2.Виноградов, Иван Матвеевич**.** Основы теории чисел: - / И. М. Виноградов. Электрон. дан. Москва : Юрайт, 2022 123 с. (Антология мысли) URL: https://urait.ru/bcode/493846 (дата обращения: 21.09.2022).Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей https://urait.ru/bcode/493846 ISBN 978-5-534-12085-1 : 329.00

3. Ниссенбаум О.В. Теоретико-числовые методы в криптографии: сб. заданий: учеб.-метод. пособие, Ч.2. - Тюмень: Изд-во ТюмГУ. - 2012. – 40 с. 4. Ниссенбаум О.В. Теоретико-числовые методы в криптографии: сб. заданий: учеб.- метод. пособие, Ч.3. - Тюмень: Изд-во ТюмГУ. - 2014. – 40 с.

Дополнительная литература:

1.Нестерова, Лариса Юрьевна. Теория чисел: учебник и практикум для вузов / Л. Ю. Нестерова, С. В. Напалков. Электрон. дан. Москва: Юрайт, 2022 150 с. (Высшее образование) URL: https://urait.ru/bcode/497147 (дата обращения: 21.09.2022). Режим доступа: Электронно-библиотечная система Юрайт, для авториз. Пользователей https://urait.ru/bcode/497147 ISBN 978-5-534-14921-0 : 549.00

5.2 Электронные образовательные 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/

6. Современные профессиональные базы данных и информационные справочные системы:

- **http://www.iacr.org** **–** ресурс Международной ассоциации криптографических исследований

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 семинарского типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная.

Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
Широких А. В..

Технологии и методы программирования

Рабочая программа для обучающихся
по специальности 10.05.01
«Компьютерная безопасность»
специализация «Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)»
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-7*

Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Технологии и методы программирования 1

В результате освоения дисциплины студент должен

Знать

- основные типы программного обеспечения
- основные компьютерные технологии
- основы разработки программного обеспечения в среде Delphi
- основы разработки Win32-приложений
- основы разработки сервисов Windows
- основы разработки .NET-приложений
- основы разработки приложений для Windows Scripting Host
- основы разработки VBA приложений
- основы разработки WEB-приложений под управлением IIS .

Уметь

- формализовать поставленную задачу
- разрабатывать эффективные алгоритмы и программы
- корректно использовать алгоритмы и технологии
- проводить выбор типа программного обеспечения, наиболее подходящего для решения поставленной задачи .

Владеть

- программной терминологией
- терминологией ООП
- навыками программной реализации различных видов ПО
- навыками использования и разработки структур данных
- навыками анализа, оценки и способов устранения типовых угроз ПО .

Технологии и методы программирования 2

В результате освоения дисциплины студент должен

Знать

- основные типы программного обеспечения
- основные компьютерные технологии
- основы разработки программного обеспечения в среде Delphi
- основы разработки Win32-приложений
- основы разработки сервисов Windows

- основы разработки .NET-приложений
- основы разработки приложений для Windows Scripting Host
- основы разработки VBA приложений
- основы разработки WEB-приложений под управлением IIS .

Уметь

- формализовать поставленную задачу
- разрабатывать эффективные алгоритмы и программы
- корректно использовать алгоритмы и технологии
- проводить выбор типа программного обеспечения, наиболее подходящего для решения поставленной задачи .

Владеть

- программной терминологией
- терминологией ООП
- навыками программной реализации различных видов ПО
- навыками использования и разработки структур данных
- навыками анализа, оценки и способов устранения типовых угроз ПО .

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**	
			5	6
Общая трудоемкость	**зач. ед.**	8	4	4
	час	288	144	144
Из них:				
Часы аудиторной работы (всего):		128	64	64
Лекции		64	32	32
Практические занятия		0	0	0
Лабораторные / практические занятия по подгруппам		64	32	32
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		160	80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный зачет	Дифференцированный зачет

3. Содержание дисциплины

Таблица 2

№	Тематика учебных встреч	Виды аудиторной работы (в ак.час.)			Итого аудиторных ак.часов по теме
		Лекции	занятия П	практические занятия Лабораторные / практическио подгруппам	
1	2	3	4	5	6
	Часов в 5 семестре	32	0	32	64
	Технологии и методы программирования 1	32	0	32	64
1	Введение	2	0	0	2
2	Лабораторное занятие	0	0	2	2
3	Введение (продолжение)	2	0	0	2
4	Лабораторное занятие	0	0	2	2
5	Основные типы программного обеспечения	2	0	0	2
6	Лабораторное занятие	0	0	2	2
7	Основные типы программного обеспечения (продолжение)	2	0	0	2
8	Лабораторное занятие	0	0	2	2
9	Обзор современных компьютерных технологий	2	0	0	2
10	Лабораторное занятие	0	0	2	2
11	Обзор современных компьютерных технологий (продолжение)	2	0	0	2
12	Лабораторное занятие	0	0	2	2
13	Разработка Win32 приложений	2	0	0	2
14	Лабораторное занятие	0	0	2	2
15	Разработка Win32 приложений (продолжение)	2	0	0	2
16	Лабораторное занятие	0	0	2	2
17	VBScript и JavaScript	2	0	0	2
18	Лабораторное занятие	0	0	2	2
19	VBA приложения	2	0	0	2
20	Лабораторное занятие	0	0	2	2
21	Синхронизация доступа	2	0	0	2
22	Лабораторное занятие	0	0	2	2
23	Работа с проецируемой памятью	2	0	0	2
24	Лабораторное занятие	0	0	2	2

25	Разработка и использование COM объектов	2	0	0	2

26	Лабораторное занятие	0	0	2	2
27	Разработка и использование COM объектов (продолжение)	2	0	0	2
28	Лабораторное занятие	0	0	2	2
29	Разработка и использование ActiveX объектов	2	0	0	2
30	Лабораторное занятие	0	0	2	2
31	Разработка и использование ActiveX объектов (продолжение)	2	0	0	2
32	Лабораторное занятие	0	0	2	2
33	Консультация	0	0	0	0
34	Дифференцированный зачет	0	0	0	0
	Часов в 6 семестре	32	0	32	64
	Технологии и методы программирования 2	32	0	32	64
1	Разработка .NET-приложений	2	0	0	2
2	Лабораторное занятие	0	0	2	2
3	Использование журнала событий	2	0	0	2
4	Лабораторное занятие	0	0	2	2
5	Разработка сервисных приложений	2	0	0	2
6	Лабораторное занятие	0	0	2	2
7	Разработка сервисных приложений (продолжение)	2	0	0	2
8	Лабораторное занятие	0	0	2	2
9	Сетевое программирование	2	0	0	2
10	Лабораторное занятие	0	0	2	2
11	Сетевое программирование (продолжение)	2	0	0	2
12	Лабораторное занятие	0	0	2	2
13	Разработка сетевых служб.	2	0	0	2
14	Лабораторное занятие	0	0	2	2
15	Асинхроннное выполнение	2	0	0	2
16	Лабораторное занятие	0	0	2	2
17	Асинхроннное выполнение (продолжение)	2	0	0	2
18	Лабораторное занятие	0	0	2	2
19	Разработка внешних UDF для баз данных	2	0	0	2
20	Лабораторное занятие	0	0	2	2
21	Разработка внешних UDF для баз данных (продолжение)	2	0	0	2
22	Лабораторное занятие	0	0	2	2
23	Веб приложения	2	0	0	2

24	Лабораторное занятие	0	0	2	2
25	Разработка приложений с использованием HttpListener.	2	0	0	2
26	Лабораторное занятие	0	0	2	2
27	Разработка asp.net приложений.	2	0	0	2
28	Лабораторное занятие	0	0	2	2
29	Обеспечение безопасности web приложений	2	0	0	2
30	Лабораторное занятие	0	0	2	2
31	Разработка веб служб	2	0	0	2
32	Лабораторное занятие	0	0	2	2
33	Консультация	0	0	0	0
34	Дифференцированный зачет	0	0	0	0
	Итого (ак.часов)	64	0	64	128

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. 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: 02.02.2022). – 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: 02.02.2022). – 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: 02.02.2022). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:

1. Научная электронная библиотека. URL: http://elibrary.ru/.
2. Электронные ресурсы ИБЦ ТюмГУ. URL: https://bmk.utmn.ru/ru/.

6. 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

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

- MS Office, платформа для электронного обучения Microsoft Teams.
- Microsoft Imagine Academy (ранее Dreamspark): ОС семейства MS Windows (редакция Pro/Server);

- Microsoft Visual Studio 19 или выше,
- IIS 7.0 или выше
- Embarcadero / Borland Delphi
- Lazarus (32 битная версия)

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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры по количеству обучающихся.

Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры.

При выполнении работ на компьютерах в учебных аудиториях студенты должны иметь возможность устанавливать, удалять, запускать и останавливать службы Windows и COM/ActiveX объекты.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
Т.И. Паюсова

Управление информационной безопасностью

Рабочая программа
для обучающихся по специальности
10.05.01. Компьютерная безопасность
специализация Безопасность компьютерных систем и сетей
(связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-1*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

В результате освоения дисциплины "Управление информационной безопасностью" обучающийся должен

Знать:

- основные задачи и понятия ИБ;
- основные стандарты, регламентирующие управление ИБ;
- принципы разработки процессов управления ИБ;
- подходы к интеграции СУИБ в общую систему управления предприятием

Уметь:

- анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ;
- определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;
- применять процессный подход к управлению ИБ в различных сферах деятельности;
- используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;
- практически решать задачи формализации разрабатываемых процессов управления ИБ;
- разрабатывать и внедрять СУИБ и оценивать ее эффективность.

Владеть:

- терминологией и процессным подходом построения систем управления ИБ;
- навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;
- навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			10
Общая трудоемкость	**зач. ед.**	4	4
	час	144	144
Из них:			
Часы аудиторной работы (всего):		60	60
Лекции		30	30
Практические занятия		30	30
Лабораторные / практические занятия по подгруппам		0	0

Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося	84	84
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)		Дифф. 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 10 семестре	30	30	0	60
	Управление информационной безопасностью	30	30	0	60
1	Введение. Базовые вопросы управления ИБ. Процессный подход	2	0	0	2
2	Введение. Базовые вопросы управления ИБ. Процессный подход	0	2	0	2
3	Введение. Базовые вопросы управления ИБ. Процессный подход	2	0	0	2
4	Введение. Базовые вопросы управления ИБ. Процессный подход	0	2	0	2
5	Область деятельности СУИБ.	2	0	0	2
6	Разработка и управление политикой ИБ информационной системы	0	2	0	2
7	Ролевая структура СУИБ. Политика СУИБ	2	0	0	2
8	Разработка и управление политикой ИБ информационной системы	0	2	0	2
9	Рискология ИБ	2	0	0	2
10	Анализ модели угроз ИБ и уязвимостей	0	2	0	2
11	Консультация	0	0	0	0
12	Рискология ИБ	2	0	0	2
13	Анализ модели информационных потоков	0	2	0	2
14	Основные процессы СУИБ.	2	0	0	2
15	.Основные процессы СУИБ	0	2	0	2
16	Основные процессы СУИБ	2	0	0	2
17	.Основные процессы СУИБ.	0	2	0	2
18	Эксплуатация и независимый аудит СУИБ	2	0	0	2
19	Эксплуатация и независимый аудит СУИБ	0	2	0	2

20	Эксплуатация и независимый аудит СУИБ	2	0	0	2
21	Эксплуатация и независимый аудит СУИБ	0	2	0	2
22	Консультация	0	0	0	0
23	Внедрение разработанных процессов	2	0	0	2
24	Внедрение разработанных процессов. Документ «Положение о применимости»	0	2	0	2
25	Документ «Положение о применимости»	2	0	0	2
26	Внедрение разработанных процессов. Документ «Положение о применимости»	0	2	0	2
27	Процесс «Управление инцидентами ИБ».	2	0	0	2
28	Процесс «Управление инцидентами ИБ»	0	2	0	2
29	Процесс «Обеспечение непрерывности ведения бизнеса»	2	0	0	2
30	Процесс «Обеспечение непрерывности ведения бизнеса»	0	2	0	2
31	Обеспечение соответствия требованиям законодательства РФ	2	0	0	2
32	Обеспечение соответствия требованиям законодательства РФ.	0	2	0	2
	Итого (ак.часов)	30	30	0	60

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 дифференцированный зачет (6 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вешах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

2. Белоус, А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения : практическое пособие / А. И. Белоус. - Москва ; Вологда : Инфра-Инженерия, 2020. - 644 с. - ISBN 978-5-9729-0512-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167734 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

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: 31.08.2022). – Режим доступа: по подписке.

4. Клименко, И.С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651 (дата обращения: дата обращения: 31.08.2022). – Режим доступа: по подписке.

5. Мосолов, А.С. Компьютерные технологии и методы проектирования в сфере безопасности : учебник для вузов / А. С. Мосолов, Н. И. Акинин. — Санкт-Петербург : Лань, 2021. — 444 с. — ISBN 978-5-8114-8034-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183115 (дата обращения: 31.08.2022). — Режим доступа: для авториз. пользователей.

6. Сычев, Ю.Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование:

Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:

- Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [On-line] (дата обращения: 31.08.2022).

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека. URL: https://rusneb.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.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместителем директора
института Переваловой М.Н.
РАЗРАБОТЧИК(И)
Шабалин А. М.

Управление инцидентами и администрирование систем защиты от утечек конфиденциальной информации

Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01. Компьютерная безопасность
Специализация: Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ОПК-16

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Управление инцидентами и администрирование систем защиты от утечек конфиденциальной информации

Знания:

- различные типы сервисов, обслуживанием которых занимается аналитик;
- ресурсы, которые нужны для детектирования и предотвращения киберугроз;
- принципы работы SIEM и DLP;
- основные распространенные технологии безопасности конечный устройств;
- функции и возможности операционных систем Windows и Linux по мониторингу инцидентов.

Умения:

- устанавливать и настраивать серверную и клиентскую части DLP-системы;
- устанавливать и настраивать серверную часть SIEM-системы;
- настраивать клиентские операционные системы Windows и Linux для отправки событий информационной безопасности на SIEM;
- настраивать ограничения для утечек конфиденциальной информации;
- определять шаблоны подозрительного поведения в SIEM;
- проводить расследование инцидентов безопасности в SOC.

.

Навыки:

- определять векторы распространенных известных атак;
- использовать современные средства операционных систем в локальной сети для выявления компьютерных атак;
- выявлять вредоносную активность и утечки конфиденциальной информации в компьютерной сети.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			10
Общая трудоемкость	**зач. ед.**	4	4
	час	144	144
Из них:			
Часы аудиторной работы (всего):		60	60
Лекции		30	30
Практические занятия		0	0

Лабораторные / практические занятия по подгруппам	30	30
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося	84	84
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 10 семестре	30	0	30	60
	Управление инцидентами и администрирование систем защиты от утечек конфиденциальной информации	30	0	30	60
1	Лекционное занятие 1	2	0	0	2
2	Лабораторное занятие 1	0	0	2	2
3	Лекционное занятие 2	2	0	0	2
4	Лабораторное занятие 2	0	0	2	2
5	Лекционное занятие 3	2	0	0	2
6	Лабораторное занятие 3	0	0	2	2
7	Лекционное занятие 4	2	0	0	2
8	Лабораторное занятие 4	0	0	2	2
9	Консультация 1	0	0	0	0
10	Лекционное занятие 5	2	0	0	2
11	Лабораторное занятие 5	0	0	2	2
12	Лекционное занятие 6	2	0	0	2
13	Лабораторное занятие 6	0	0	2	2
14	Лекционное занятие 7	2	0	0	2
15	Лабораторное занятие 7	0	0	2	2
16	Лекционное занятие 8	2	0	0	2
17	Лабораторное занятие 8	0	0	2	2
18	Консультация 2	0	0	0	0
19	Лекционное занятие 9	2	0	0	2
20	Лабораторное занятие 9	0	0	2	2
21	Лекционное занятие 10	2	0	0	2
22	Лабораторное занятие 10	0	0	2	2
23	Лекционное занятие 11	2	0	0	2
24	Лабораторное занятие 11	0	0	2	2
25	Лекционное занятие 12	2	0	0	2
26	Лабораторное занятие 12	0	0	2	2
27	Консультация 3	0	0	0	0
28	Лекционное занятие 13	2	0	0	2
29	Лабораторное занятие 13	0	0	2	2

30	Лекционное занятие 14	2	0	0	2
31	Лабораторное занятие 14	0	0	2	2
32	Лекционное занятие 15	2	0	0	2
33	Лабораторное занятие 15	0	0	2	2
34	Консультация 4	0	0	0	0
35	Экзамен	0	0	0	0
	Итого (ак.часов)	30	0	30	60

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 экзамена.

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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Абденов А.Ж. Анализ, описание и оценка функциональных узлов SIEM-системы : учебное пособие / Абденов А.Ж., Трушин В.А., Сулайман К.. — Новосибирск : Новосибирский государственный технический университет, 2018. — 122 c. — ISBN 978-5-7782-3603-5. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/91179.html (дата обращения: 22.11.2022).
2. Пелешенко В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / Пелешенко В.С., Говорова С.В., Лапина М.А.. — Ставрополь : Северо-Кавказский федеральный университет, 2017. — 86 c. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/69405.html (дата обращения: 22.11.2022).

5.2 Электронные образовательные 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/

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека https://rusneb.ru/

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

MS Office, платформа для электронного обучения Microsoft Teams, ОС MS Windows, ОС FreeBSD.

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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.

Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
С.Г. Монтанари

Электроника и схемотехника

Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.03.01 «Информационная безопасность» профиль
«Безопасность компьютерных систем» форма
обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ОПК-4*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Электроника и схемотехника

В результате освоения дисциплины обучающийся должен:

Знать:

- терминологию и символику, используемую в электронике, методы составления и чтения основных видов электрических схем;
- основные физические понятия и принципы функционирования базовых электронных полупроводниковых компонентов в аналоговых и цифровых системах; основные параметры и принципы работы базовых функциональных элементов радиоэлектроники (усилителей, генераторов и т.п.);
- основные принципы работы и проектирования электронных систем; особенности применения аналоговых и цифровых радиоэлектронных устройств;
- основные подходы к решению практических задач, связанных с анализом сигналов в частотной области.

Уметь:

- проводить базовые теоретические и экспериментальные исследования электронного оборудования и систем;
- оценивать степень достоверности результатов, полученных с помощью экспериментальных и теоретических методов исследований;
- рассчитывать простые аналоговые и цифровые радиоэлектронные устройства;
- применять современную вычислительную технику при анализе и разработке аналоговых и цифровых электронных устройств.

Владеть:

- приемами и навыками решения конкретных задач из разных областей электроники и схемотехники;
- основными математическими методами анализа и расчета электрических цепей и сигналов;
- базовыми навыками проектирования, конструирования, монтажа и наладки простых радиоэлектронных устройств.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			6
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося		80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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 6 семестре	32	0	32	64
1	Полупроводниковые приборы.	2	0	0	2
2	Биполярные транзисторы	2	0	0	2
3	Исследование диодов	0	0	4	4
4	Полевые транзисторы, их разновидности и основные параметры.	2	0	0	2
5	Усилители	2	0	0	2
6	Исследование биполярного транзистора и усилительного каскада с общим эмиттером	0	0	4	4
7	Элементы теории обратной связи в усилителях	2	0	0	2
8	Усилительные каскады на биполярных и полевых транзисторах	2	0	0	2
9	Сдача отчетов и исправление замечаний по предыдущим работам	0	0	4	4
10	Дифференциальный усилительный каскад. Операционный усилитель.	2	0	0	2
11	Применение операционных усилителей для обработки аналоговых сигналов. Компараторы.	2	0	0	2
12	Исследование инвертирующего и неинвертирующего усилителя на операционном усилителе.	0	0	4	4

	Генераторы. LC- и RC-генераторы гармонических колебаний.	2	0	0	2
	Прохождение гармонического сигнала через нелинейную цепь.	2	0	0	2
	Исследование логических элементов цифровых интегральных схем.	0	0	4	4
	Цифровые сигналы.	2	0	0	2
	Классификация цифровых устройств.	2	0	0	2
	Исследование JK-триггера и счетчика.	0	0	4	4
	Триггеры, регистры, счетчики.	2	0	0	2
	Мультиплексоры и демультиплексоры. Кодеры и декодеры (шифраторы и дешифраторы).	2	0	0	2
	Исследование параметрического стабилизатора напряжения.	0	0	4	4
	Аналого-цифровое и цифро-аналоговое преобразования.	2	0	0	2
	Основы микропроцессорной техники.	2	0	0	2
	Сдача отчетов и исправление замечаний по предыдущим работам	0	0	4	4
	Консультация перед зачетом	0	0	0	0
	Зачет по дисциплине	0	0	0	0
	Итого (ак.часов)	32	0	32	64

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 дифференцированный зачет (6 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

2. Белоус, А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения : практическое пособие / А. И. Белоус. - Москва ; Вологда : Инфра-Инженерия, 2020. - 644 с. - ISBN 978-5-9729-0512-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167734 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

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: 31.08.2022). – Режим доступа: по подписке.

4. Клименко, И.С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651 (дата обращения: дата обращения: 31.08.2022). – Режим доступа: по подписке.

5. Мосолов, А.С. Компьютерные технологии и методы проектирования в сфере безопасности : учебник для вузов / А. С. Мосолов, Н. И. Акинин. — Санкт-Петербург : Лань, 2021. — 444 с. — ISBN 978-5-8114-8034-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183115 (дата обращения: 31.08.2022). — Режим доступа: для авториз. пользователей.

6. Сычев, Ю.Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:

- Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [Online] (дата обращения: 31.08.2022).

6. Современные профессиональные базы данных и информационные справочные системы:

Национальная электронная библиотека. URL: https://rusneb.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.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
Широких А. В.

Интернет вещей Рабочая программа

для обучающихся по направлению подготовки (специальности)
10.05.01 «Компьютерная безопасность»
специализация «Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)»
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ПК-6*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Интернет вещей

В результате освоения дисциплины студент должен

Знать

- основные типы оборудования используемого в проектах интернета вещей
- основные типы микроконтроллеров и микрокомпьютеров интернета вещей, их особенности, достоинства и недостатки
- основы разработки программного обеспечения в среде Arduino Studio
- наиболее распространенные типы сетей интернета вещей

Уметь

- формализовать поставленную задачу
- разбивать проект на функционально независимые блоки
- корректно подбирать необходимое оборудование
- разрабатывать алгоритм работы

Владеть

- терминологией Интернета Вещей
- навыками разработки решений Интернета Вещей
- навыками разработки программ (скетчей) Интернета Вещей

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			6
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося	80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)		Дифференцированный зачет

3. Содержание дисциплины

Таблица 2

№	Тематика учебных встреч	Виды аудиторной работы (в ак.час.)			Итого аудиторных ак.часов по теме
		Лекции	П	Лабораторные / практические занятия по подгруппам	
1	2	3	4	5	6
	Часов в 6 семестре	32	0	32	64
	Интернет вещей	32	0	32	64
1	Микрокомпьютеры (часть 1)	2	0	0	2
2	Лабораторное занятие 1	0	0	2	2
3	Микрокомпьютеры (часть 2)	2	0	0	2
4	Лабораторное занятие 2	0	0	2	2
5	Датчики и исполнительные устройства.	2	0	0	2
6	Лабораторное занятие 3	0	0	2	2
7	Датчики и исполнительные устройства. (продолжение)	2	0	0	2
8	Лабораторное занятие 4	0	0	2	2
9	Разработка проектов на базе Arduino	2	0	0	2
10	Лабораторное занятие 5	0	0	2	2
11	Механизмы сетевого взаимодействия устройств интернет вещей	2	0	0	2
12	Лабораторное занятие 6	0	0	2	2
13	Работа с датчиками температуры DS18B20 и другими устройствами 1Wire	2	0	0	2
14	Лабораторное занятие 7	0	0	2	2

15	Механизмы сетевого взаимодействия устройств интернет вещей (продолжение)	2	0	0	2
16	Лабораторное занятие 8	0	0	2	2
17	Особенности подключения и работы устройств 2-wire	2	0	0	2
18	Лабораторное занятие 9	0	0	2	2
19	Механизмы сетевого взаимодействия устройств интернет вещей (продолжение)	2	0	0	2
20	Лабораторное занятие 10	0	0	2	2
21	Механизмы сетевого взаимодействия устройств интернет вещей (продолжение)	2	0	0	2
22	Лабораторное занятие 11	0	0	2	2
23	Взаимодействие интернет вещей с использованием радиомодуля NRF24L01	2	0	0	2
24	Лабораторное занятие 12	0	0	2	2
25	Работа в GSM сетях	2	0	0	2
26	Лабораторное занятие 13	0	0	2	2
27	Использование проводного интернет.	2	0	0	2
28	Лабораторное занятие 14	0	0	2	2
29	Использование WiFi модулей. Работа с сетями WiFi с использованием плат WEMOS	2	0	0	2
30	Лабораторное занятие 15	0	0	2	2
31	Использование WiFi модулей. Работа с сетями WiFi с использованием плат WEMOS	2	0	0	2
32	Лабораторное занятие 15	0	0	2	2
33	Консультация	0	0	0	0
34	Дифференцированный зачет	0	0	0	0
	Итого (ак.часов)	32	0	32	64

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 дифференцированный зачет (6 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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1.Литература:

1. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вешах простыми словами
: монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 31.08.2022). – Режим доступа: по подписке.
2. Белоус, А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения : практическое пособие / А. И. Белоус. - Москва ; Вологда : Инфра-Инженерия, 2020. - 644 с. - ISBN 978-5-9729-0512-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167734 (дата обращения: 31.08.2022). – Режим доступа: по подписке.
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: 31.08.2022). – Режим доступа: по подписке.
4. Клименко, И.С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651 (дата обращения: дата обращения: 31.08.2022). – Режим доступа: по подписке.

5. Мосолов, А.С. Компьютерные технологии и методы проектирования в сфере безопасности : учебник для вузов / А. С. Мосолов, Н. И. Акинин. — Санкт-Петербург : Лань, 2021. — 444 с. — ISBN 978-5-8114-8034-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183115 (дата обращения: 31.08.2022). — Режим доступа: для авториз. пользователей.
6. Сычев, Ю.Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364 (дата обращения: 31.08.2022). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:
Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [Online]

1. Документы IETF – инженерного совета Интернета. - http://www.ietf.org/rfc.html [Online] (дата обращения: 31.08.2022).

6. Современные профессиональные базы данных и информационные справочные системы:
1. Национальная электронная библиотека. - URL: https://rusneb.ru/

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

MS Office, платформа для электронного обучения Microsoft Teams.
Arduino IDE — https://www.arduino.cc/en/software
Autodesk Tinkercad - https://tinkercad.com/

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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры по количеству обучающихся.

Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора Института
математики и компьютерных наук
М.Н. Перевалова
РАЗРАБОТЧИК(И)
Зулькарнеев И. Р.

ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Рабочая программа
для обучающихся по специальности
10.05.01 «Компьютерная безопасность»
специализация «Безопасность компьютерных систем и сетей» (связь, информационные и коммуникационные технологии)
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ПК-4

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Проектирование и внедрение систем защиты информации

В результате изучения дисциплины студент должен

Знать

- общие принципы построения и внедрения систем защиты информации для автоматизированных систем;
- необходимые для проектирования ГОСТы и НПА;
- принципы проектирования архитектуры, структуры и основных объектов защищаемых автоматизированных систем;
- основные этапы процесса проектирования и методы, используемые при построении проектируемой системы защиты информации.

Уметь

- формировать требования к проектируемой системе защиты информации с учетом анализа угроз;
- составлять функциональные схемы проектируемой СЗИ и АС.

Владеть

- методами построения защищенных автоматизированных систем;
- навыками составления, технического задания, технического проекта и пониманием содержания основных этапов процесса проектирования.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			6
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося		80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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 6 семестре	32	32	0	64
	Проектирование и внедрение систем защиты информации	32	32	0	64
1	Лекция 1.	2	0	0	2
2	Практика 1	0	2	0	2
3	Лекция 2.	2	0	0	2
4	Практика 2	0	2	0	2
5	Лекция 3.	2	0	0	2
6	Практика 3	0	2	0	2
7	Лекция 4.	2	0	0	2
8	Практика 4	0	2	0	2
9	Лекция 5.	2	0	0	2
10	Практика 5	0	2	0	2
11	Лекция 6.	2	0	0	2
12	Практика 6	0	2	0	2
13	Лекция 7.	2	0	0	2
14	Практика 7	0	2	0	2
15	Лекция 8.	2	0	0	2
16	Практика 8	0	2	0	2
17	Лекция 9.	2	0	0	2
18	Практика 9	0	2	0	2
19	Лекция 10	2	0	0	2
20	Практика 10	0	2	0	2
21	Лекция 11.	2	0	0	2
22	Практика 11	0	2	0	2
23	Лекция 12.	2	0	0	2
24	Практика 12	0	2	0	2
25	Лекция 13.	2	0	0	2
26	Практика 13	0	2	0	2
27	Лекция 14.	2	0	0	2
28	Практика 14	0	2	0	2
29	Лекция 15.	2	0	0	2
30	Практика 1	0	2	0	2
31	Лекция 16.	2	0	0	2

32	Практика 16	0	2	0	2
33	Консультация	0	0	0	0
34	Зачет с оценкой	0	0	0	0
	Итого (ак.часов)	32	32	0	64

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 устного 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. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков [и др.].. — Брянск : Брянский государственный технический университет, 2012. — 224 c. — ISBN 978-89838-488-3. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/7007.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.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора Института
математики и компьютерных наук
Перевалова М.Н.
РАЗРАБОТЧИК
Пуртов В. Г.

Разработка и защита мобильных приложений
Рабочая программа
для обучающихся по направлению подготовки (специальности)
10.05.01 Компьютерная безопасность
Профиль: Безопасность компьютерных систем и сетей
(связь, информационные и коммуникационные технологии)
Форма обучения: очная

Тюменский государственный университет
2022

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ПК-5

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Разработка и защита мобильных приложений

В результате освоения дисциплины студент должен

Знать:

• этапы и тенденции развития программирования, способы применения ИТ при разработке мобильных приложений.

• особенности применения сервисных программ и оболочек при разработке мобильных приложений.

• содержание рынка программных продуктов и информационных услуг, тенденции, развитие и особенности рынка.

Уметь:

• выбрать оптимальный программный продукт и модели информационных технологий из нескольких возможных для решения прикладной задачи, и провести сравнительную оценку эффективности.

• выбрать программный продукт и технологии для решения задачи с учетом конкретной предметной области и провести анализ эффективности использования ПО для решения задач в предметной области.

• разрабатывать сервисные программы и сервисные оболочки при разработке мобильных приложений с учетом конкретной предметной области.

Иметь навыки:

• применения информационных технологий и творческого подхода при решении стандартных и нестандартных задач

• выбора программных продуктов и мобильных технологий для решения задачи.

• использования сервисных программ и сервисных оболочек при разработке мобильных приложений для решения задачи.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			7
Общая трудоемкость	**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 консультации, иную контактную работу и самостоятельную работу обучающегося	80	80
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)		Дифференцированный 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	32	0	32	64
	Разработка и защита мобильных приложений	32	0	32	64
1	Введение	2	0	0	2
2	Лабораторное занятие	0	0	2	2
3	Введение (продолжение)	2	0	0	2
4	Лабораторное занятие	0	0	2	2
5	Архитектура приложений для Android	2	0	0	2
6	Лабораторное занятие	0	0	2	2
7	Архитектура приложений для Android (продолжение)	2	0	0	2
8	Лабораторное занятие	0	0	2	2
9	Основы разработки интерфейсов мобильных приложений	2	0	0	2
10	Лабораторное занятие	0	0	2	2
11	Основы разработки интерфейсов мобильных приложений (продолжение)	2	0	0	2
12	Лабораторное занятие	0	0	2	2
13	Основы разработки многооконных приложений	2	0	0	2
14	Лабораторное занятие	0	0	2	2
15	Основы разработки многооконных приложений (продолжение)	2	0	0	2
16	Лабораторное занятие	0	0	2	2
17	Использование возможностей смартфона в приложениях	2	0	0	2
18	Лабораторное занятие	0	0	2	2
19	Использование возможностей смартфона в приложениях (продолжение)	2	0	0	2
20	Лабораторное занятие	0	0	2	2
21	Использование библиотек	2	0	0	2
22	Лабораторное занятие	0	0	2	2

23	Использование библиотек (продолжение)	2	0	0	2
24	Лабораторное занятие	0	0	2	2
25	Работа с базами данных, графикой и анимацией	2	0	0	2
26	Лабораторное занятие	0	0	2	2
27	Работа с базами данных, графикой и анимацией (продолжение)	2	0	0	2
28	Лабораторное занятие	0	0	2	2
29	Консультация	0	0	0	0
30	Инструменты для разработки и их установка	2	0	0	2
31	Лабораторное занятие	0	0	2	2
32	Консультация	0	0	0	0
33	Инструменты для разработки и их установка (продолжение)	2	0	0	2
34	Лабораторное занятие	0	0	2	2
35	Консльтация	0	0	0	0
36	Дифференцированный зачет	0	0	0	0
	Итого (ак.часов)	32	0	32	64

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. Дифференцированный зачет проходит по билетам. В билете - 2 вопроса.

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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 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. — 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
2. 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.

5.2 Электронные образовательные 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/

6. Современные профессиональные базы данных и информационные справочные системы:

- Национальная электронная библиотека. URL: https://rusneb.ru/
- Institute of Electrical and Electronics. URL:

https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true Engineers, Inc (IEEE)

- Межвузовская электронная библиотека (МЭБ). URL: https://icdlib.nspu.ru/

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

MS Office, платформа для электронного обучения Microsoft Teams. Среда разработки Visual Studio с установленным фреймворком Xamarin, эмулятор устройств на платформе Android, среда разработки Android Studio

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.

Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
Перевалова М.Н.
РАЗРАБОТЧИК
Оленников А. А.

РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Рабочая программа для
обучающихся по специальности
10.05.01. Компьютерная
безопасность
специализация «Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)»
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля): ПК-2, ПК-3.*

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

В результате освоения ОП выпускник должен обладать следующими компетенциями: Способен администрировать процесс управления безопасностью сетевых устройств и программного обеспечения (ПК-2);

 Способен выполнять комплекс мер по обеспечению функционирования СССЭ (за исключением сетей связи специального назначения) и средств их защиты от НСД (ПК-3).

В результате освоения ОП выпускник должен:

знать:

- нормативно-техническую документацию;
- принцип работы оборудования автоматизированных систем;
- программное обеспечение для моделирования технологических процессов;
- способы проведения анализа, а также подбора оборудования и средств защиты для предложенного технологического процесса; • методики чтения технологических схем;
- программное обеспечение для проектирования схем автоматизированных систем и узлов

уметь:

- работать с нормативно-технической документацией;
- применять навыки для проведения анализа, а также подбора оборудования и средств защиты для предложенного технологического процесса;
- анализировать предложенные структурные и принципиальные технологические схемы и сети автоматизированных систем и узлов;
- работать с программным обеспечением для проектирования схем автоматизированных систем и узлов;
- проводить экспериментально-исследовательские работы с оборудованием и сетями автоматизированных систем.

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):		60	60
Лекции		30	30
Практические занятия		0	0
Лабораторные / практические занятия по подгруппам		30	30
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		84	84
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)			Дифференцированный 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 / практическио подгруппам	
1	2	3	4	5	6
	Часов в 10 семестре	30	0	30	60
	Разработка и эксплуатация автоматизированных систем в защищенном исполнении	30	0	30	60
1	Лекционное занятие 1	2	0	0	2
2	Лабораторная работа 1. Построение структурных схем.	0	0	2	2
3	Лекционное занятие 2	2	0	0	2
4	Лабораторная работа 2. Подбор датчиков и контроллера узла учета тепловой энергии.	0	0	2	2
5	Лекционное занятие 3	2	0	0	2
6	Лабораторная работа 3. Работа с тепловычислителем ТСР-010.	0	0	2	2
7	Лекционное занятие 4	2	0	0	2
8	Лабораторная работа 4. Разработка модели угроз системы погодного регулирования.	0	0	2	2
9	Лекционное занятие 5	2	0	0	2
10	Лабораторная работа 5. Разработка алгоритмов и мероприятий по безаварийной работе теплового системы погодного регулирования и тепловычислителя.	0	0	2	2
11	Лекционное занятие 6	2	0	0	2
12	Лабораторная работа 6. Настройка контроллера СУНА на требуемые режимы работы.	0	0	2	2
13	Лекционное занятие 7	2	0	0	2

14	Лабораторная работа 7. Работа с адресной видеокамерой и видеорегистратором, и их настройками.	0	0	2	2
15	Лекционное занятие 8	2	0	0	2
16	Лабораторная работа 8. Работа в среда проектирования Codesys.	0	0	2	2
17	Лекционное занятие 9	2	0	0	2
18	Лабораторная работа 9. Работа в среда проектирования Codesys.	0	0	2	2
19	Лекционное занятие 10	2	0	0	2
20	Лабораторная работа 10. Построение и защита технологической сети.	0	0	2	2
21	Лекционное занятие 11	2	0	0	2
22	Лабораторная работа 11. Разработка Скада-системы.	0	0	2	2
23	Лекционное занятие 12	2	0	0	2
24	Лабораторная работа 12. Разработка Скада-системы.	0	0	2	2
25	Лекционное занятие 13	2	0	0	2
26	Лабораторная работа 13. Настройка виртуализации серверов.	0	0	2	2
27	Лекционное занятие 14	2	0	0	2
28	Лабораторная работа 14. Оранизация защиты сети.	0	0	2	2
29	Лекционное занятие 15	2	0	0	2
30	Лабораторная работа 15. Оранизация защиты сети. Настройка сетвого оборудования и контроллеров.	0	0	2	2
31	Консультация перед зачетом	0	0	0	0
32	Дифференцированный зачет	0	0	0	0
	Итого (ак.часов)	30	0	30	60

4. Система оценивания.

В 9 семестре предусмотрен дифференцированный зачет. Зачет с оценкой является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и 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 зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных 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 90% лабораторных 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 лабораторные 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 оценку, полученную в рамках модульнорейтинговой системы, имеет право на сдачу зачета или выполнение дополнительного задания на усмотрение преподавателя.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература

1 Методологические основы построения защищенных автоматизированных систем : учебное пособие / А. В. Душкин, О. В. Ланкин, С. В. Потехецкий [и др.]. — Воронеж : Воронежский государственный университет инженерных технологий, 2013. — 260 с. — ISBN 978-5-89448-981-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/47427.html (дата обращения: 20.09.2022). — Режим доступа: для авторизир. пользователей.

2 Рябцев, В. Г. Автоматизация технических систем специальных объектов : учебнометодическое пособие / В. Г. Рябцев. - Волгоград : ФГБОУ ВО Волгоградский ГАУ, 2019. - 84 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1087883 (дата обращения: 20.09.2022). – Режим доступа: по подписке.

3 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 9785-369-01450-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/763644 (дата обращения: 20.09.2022). – Режим доступа: по подписке.

5.2 Электронные образовательные ресурсы:

1. Научная электронная библиотека. URL: http://elibrary.ru/.
2. Электронные ресурсы ИБЦ ТюмГУ. URL: https://bmk.utmn.ru/ru/.

6. 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

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

- MS Office, платформа для электронного обучения Microsoft Teams.
- 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);

  Программное обеспечение виртуализации: VirtualBox (бесплатная лицензия доступна: https://www.virtualbox.org/wiki/Downloads).

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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер.
- Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Заместитель директора ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И) Широких
А. В.

Защита программ и данных

Рабочая программа для обучающихся
по специальности 10.05.01
«Компьютерная безопасность»
специализация «Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)»
форма обучения очная

1. Планируемые результаты освоения дисциплины

1.1. Компетенции обучающегося, формируемые в результате освоения данной дисциплины *(модуля):* ОПК-8, ОПК-10

1.2. Индикаторы достижения компетенций, соотнесенные с планируемыми результатами обучения:

Защита программ и данных

В результате освоения дисциплины студент должен

Знать

- понятия процессор, машинные команды, оперативная память, регистры, смещение, сегмент, разрядность, прерывание,
- основные машинные команды сложения (8086)
- основные машинные команды вычитания (8086)
- основные машинные команды умножения(8086)
- основные машинные команды деления (8086)
- основные машинные команды битовой арифметики (8086)
- низкоуровневой адресации (8086)
- знать способы создания побочных эффектов программы, позволяющие скрыть затруднить отладку
- современные средства защиты ПО
- основные виды закладок ПО
- основные способы анализа ПО.

Уметь

- разрабатывать простые программы на языке ассемблер
- понимать логику работы программы на языке ассемблер
- определять основные побочные эффекты программы, позволяющие скрыть затруднить отладку
- использовать современные средства защиты ПО.

Владеть

- методами создания побочных эффектов программы, позволяющие скрыть затруднить отладку
- современными методами защиты ПО
- методами отладки и анализа ПО.

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы		**Всего часов**	**Кол-во часов в семестре (ак.ч.)**
			9
	зач. ед.	4	4

Общая трудоемкость	**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 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 / практическио подгруппам	
1	2	3	4	5	6
	Часов в 9 семестре	32	0	32	64
	Защита программ и данных	32	0	32	64
1	Введение в анализ ПО	2	0	0	2
2	Лабораторное занятие 1	0	0	2	2
3	Введение в анализ ПО	2	0	0	2
4	Лабораторное занятие 2	0	0	2	2
5	Статический и динамический методы анализа ПО	2	0	0	2
6	Лабораторное занятие 3	0	0	2	2
7	Статический и динамический методы анализа ПО	2	0	0	2
8	Лабораторное занятие 4	0	0	2	2
9	Статический и динамический методы анализа ПО	2	0	0	2
10	Лабораторное занятие 5	0	0	2	2
11	Статический и динамический методы анализа ПО	2	0	0	2
12	Лабораторное занятие 6	0	0	2	2
13	Особенности анализа некоторых видов ПО	2	0	0	2
14	Лабораторное занятие 7	0	0	2	2
15	Особенности анализа некоторых видов ПО	2	0	0	2
16	Лабораторное занятие 8	0	0	2	2
17	Инструменты анализа ПО	2	0	0	2
18	Лабораторное занятие 9	0	0	2	2
19	Инструменты анализа ПО	2	0	0	2
20	Лабораторное занятие 10	0	0	2	2
21	Защита программ от анализа	2	0	0	2
22	Лабораторное занятие 11	0	0	2	2

23	Защита программ от анализа	2	0	0	2
24	Лабораторное занятие 12	0	0	2	2
25	Программные закладки	2	0	0	2
26	Лабораторное занятие 13	0	0	2	2
27	Программные закладки.	2	0	0	2
28	Лабораторное занятие 14	0	0	2	2
29	Модели взаимодействия программных закладок с атакуемой системой	2	0	0	2
30	Лабораторное занятие 15	0	0	2	2
31	Методы внедрения программных закладок.	2	0	0	2
32	Лабораторное занятие 17	0	0	2	2
33	Консультация	0	0	0	0
34	Экзамен	0	0	0	0
	Итого (ак.часов)	32	0	32	64

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 экзамена.

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».

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Литература:

1. Крис, Касперски Фундаментальные основы хакерства. Искусство дизассемблирования / Касперски Крис. — Москва : СОЛОН-Р, 2016. — 446 c. — ISBN 5-93455-175-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/90401.html (дата обращения: 25.11.2022)

5.2 Электронные образовательные ресурсы:

2. Научная электронная библиотека. URL: http://elibrary.ru/.
3. Электронные ресурсы ИБЦ ТюмГУ. URL: https://bmk.utmn.ru/ru/.
4.

6. 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

7. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

- MS Office, платформа для электронного обучения Microsoft Teams.
- 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. Программное обеспечение виртуализации: VirtualBox (бесплатная лицензия доступна: https://www.virtualbox.org/wiki/Downloads).
- Операционная система FreeDOS (бесплатная лицензия доступна: https://ru.wikipedia.org/wiki/FreeDOS).

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 лабораторного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры по количеству обучающихся.

Аудитория для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры.