ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

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

Сети и системы передачи информации

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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-1.2*

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
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 4 семестре	32	0	32	64
	Сети и системы передачи информации	32	0	32	64
1	Лекция 1	2	0	0	2
2	Лекция 2	2	0	0	2
3	Лабораторное занятие 1	0	0	2	2
4	Лекция 3	2	0	0	2
5	Лабораторное занятие 2	0	0	2	2
6	Лекция 4	2	0	0	2
7	Лабораторное занятие 3	0	0	2	2
8	Лекция 5	2	0	0	2
9	Лабораторное занятие 4	0	0	2	2
10	Лекция 6	2	0	0	2
11	Лабораторное занятие 5	0	0	2	2
12	Лекция 7	2	0	0	2
13	Лабораторное занятие 6	0	0	2	2
14	Лекция 8	2	0	0	2
15	Лабораторное занятие 7	0	0	2	2
16	Лекция 9	2	0	0	2
17	Лабораторное занятие 8	0	0	2	2
18	Лекция 10	2	0	0	2
19	Лабораторное занятие 9	0	0	2	2
20	Лекция 11	2	0	0	2
21	Лабораторное занятие 10	0	0	2	2
22	Консультация 1	0	0	0	0
23	Лекция 12	2	0	0	2
24	Лабораторное занятие 11	0	0	2	2
25	Лекция 13	2	0	0	2
26	Лабораторное занятие 12	0	0	2	2
27	Лекция 14	2	0	0	2
28	Лабораторное занятие 12	0	0	2	2
29	Лекция 15	2	0	0	2
30	Лабораторное занятие 13	0	0	2	2
31	Лекция 16	2	0	0	2
32	Лабораторное занятие 13	0	0	2	2

33	Лабораторное занятие 14	0	0	2	2
34	Консультация 2	0	0	0	0
35	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 (4 семестр), экзамен (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 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)
Е.А. Оленников

Администрирование операционных систем

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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-1.4*

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

Администрирование операционных систем

В результате изучения дисциплины студент должен:

знать:

- 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.

уметь:

- выполнять установку и конфигурирование ОС Windows, Linux, Unix;
- выполнять задачи по управлению пользователями в ОС Windows, Linux, Unix;
- выполнять задачи по управлению запоминающими устройствами в ОС Windows, Linux, Unix;
- выполнять задачи по ограничению доступа к объектам файловой системы в ОС Windows, Linux, Unix;
- конфигурировать и администрировать основные сетевые службы в ОС Windows, Linux, Unix;
- 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.

иметь 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
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 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
	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 (5 семестр), экзамен (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 ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
М.Б. Атманских

Дополнительные главы математики

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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 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)
И.Р. Зулькарнеев

Организационное и правовое обеспечение информационной безопасности

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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:

Организационное и правовое обеспечение информационной безопасности

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

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.

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 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)
А.А. Оленников

Разработка и защита web-приложений

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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

В результате освоения дисциплины студент должен

Знать

- принципы функционирования веб-приложений;
- наиболее распространённые web-сервера, их возможности и функционал;
- механизмы обеспечения безопасности веб-приложений;
- наиболее распространенные типы уязвимостей.

Уметь

- разрабатывать основные типы веб-приложений для наиболее распространённых web-серверов;
- производить анализ защищенности веб-приложения;
- производить защиту веб-приложения;
- производить устранение основных типов угроз.

Владеть

- терминологией веб-приложений;
- навыками разработки веб-приложений;
- навыками разработки безопасных веб-приложений для различных применений.

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)		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	0	32	64
	Разработка и защита web-приложений	32	0	32	64
1	Введение	2	0	0	2
2	Лабораторное занятие 1	0	0	2	2
3	Введение	2	0	0	2
4	Лабораторное занятие	0	0	2	2
5	CSS	2	0	0	2
6	Лабораторное занятие	0	0	2	2
7	CSS ч.2	2	0	0	2
8	Лабораторное занятие	0	0	2	2
9	Отправка форм	2	0	0	2
10	Лабораторное занятие	0	0	2	2
11	Идентификация, Аутентификация, Авторизация	2	0	0	2
12	Лабораторное занятие	0	0	2	2
13	JavaScript ч.1	2	0	0	2
14	Лабораторное занятие	0	0	2	2
15	Javascript ч.2	2	0	0	2
16	Лабораторное занятие	0	0	2	2
17	Javascript 3ч.	2	0	0	2
18	Лабораторное занятие	0	0	2	2
19	PHP ч.1	2	0	0	2
20	Лабораторное занятие	0	0	2	2
21	PHP ч.2	2	0	0	2
22	Лабораторное занятие	0	0	2	2
23	PHP ч.3. ООП	2	0	0	2
24	Лабораторное занятие	0	0	2	2
25	PHP ч.4. MVC	2	0	0	2
26	Лабораторное занятие	0	0	2	2
27	Фреймворки, CMS	2	0	0	2
28	Лабораторное занятие	0	0	2	2
29	Веб-сервер	2	0	0	2
30	Лабораторное занятие	0	0	2	2
31	Веб-сервер	2	0	0	2

32	Лабораторное занятие	0	0	2	2
33	Консультация	0	0	0	0
34	Аттестация 1	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 (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 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)
О.А. Нестерова

Системы управления базами данных

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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:

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 *экзамен (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 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)
А.В. Широких

Технологии и методы программирования

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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:

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
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 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
	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 (5-6 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 ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
М.Б. Атманских

Дополнительные главы математической статистики

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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 [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)
А.В. Широких

Интернет вещей

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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:

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	Практические занятия	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 1-Wire	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 [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

Основы управления информационной безопасностью

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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:

Основы управления информационной безопасностью

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.)**
			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
	Основы управления информационной безопасностью	32	32	0	64
1	Введение. Базовые вопросы управления ИБ. Процессный подход	4	0	0	4
2	Введение. Базовые вопросы управления ИБ. Процессный подход	0	4	0	4
3	Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ	4	0	0	4
4	Разработка и управление политикой ИБ информационной системы	0	4	0	4
5	Рискология ИБ	4	0	0	4
6	Анализ модели угроз ИБ и уязвимостей	0	4	0	4
7	Основные процессы СУИБ. Обязательная документация СУИБ	4	0	0	4
8	.Основные процессы СУИБ	0	4	0	4
9	Эксплуатация и независимый аудит СУИБ	4	0	0	4
10	Эксплуатация и независимый аудит СУИБ	0	4	0	4
11	Внедрение разработанных процессов. Документ «Положение о применимости»	4	0	0	4
12	Внедрение разработанных процессов. Документ «Положение о применимости»	0	4	0	4
13	Процесс «Управление инцидентами ИБ». Процесс «Обеспечение непрерывности ведения бизнеса»	4	0	0	4
14	Процесс «Управление инцидентами ИБ»	0	4	0	4
15	Обеспечение соответствия требованиям законодательства РФ	4	0	0	4

16	Обеспечение соответствия требованиям законодательства РФ.	0	4	0	4
17	Консультация	0	0	0	0
18	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 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 [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)
С.Г. Монтанари

Электроника и схемотехника

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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:

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
	Электроника и схемотехника	32	0	32	64
1	Полупроводниковые приборы. Свойства p-n перехода. Диоды, их разновидности (стабилитроны, варикапы, туннельные диоды и др.)	2	0	0	2
2	Лекционное занятие 2	2	0	0	2
3	Лабораторное занятие 1	0	0	4	4
4	Лекционное занятие 3	2	0	0	2
5	Лекционное занятие 4	2	0	0	2
6	Лабораторное занятие 2	0	0	4	4
7	Лекционное занятие 5	2	0	0	2
8	Лекционное занятие 6	2	0	0	2
9	Лабораторное занятие 3	0	0	4	4
10	Лекционное занятие 7	2	0	0	2
11	Лекционное занятие 8	2	0	0	2
12	Лабораторное занятие 4	0	0	4	4
13	Лекционное занятие 9	2	0	0	2
14	Лекционное занятие 10	2	0	0	2
15	Лабораторное занятие 5	0	0	4	4
16	Лекционное занятие 11	2	0	0	2
17	Лекционное занятие 12	2	0	0	2
18	Лабораторное занятие 6	0	0	4	4
19	Лекционное занятие 13	2	0	0	2
20	Лекционное занятие 14	2	0	0	2
21	Лабораторное занятие 7	0	0	4	4
22	Лекционное занятие 15	2	0	0	2
23	Лекционное занятие 16	2	0	0	2
24	Лабораторное занятие 8	0	0	4	4
25	Консультация перед экзаменом	0	0	0	0
26	Аттестация 1	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 ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
Е.А. Оленников

Защита в операционных системах

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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*

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

Защита в операционных системах

В результате освоения ОП выпускник должен:

знать:

- основные понятия и положения защиты информации в ОС;
- основные угрозы ИБ в ОС;
- ресурсы, подлежащие защите;
- 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;

уметь:

- проводить анализ угроз информационной безопасности 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;

иметь 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
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 в операционных системах	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	Экзамен по ЗОС	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 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)
И.Р. Зулькарнеев

Защита государственных информационных систем и персональных данных

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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:

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.)**
			7
	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)			

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
	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.

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 (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 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)
И.И. Пряхин

Защита информации от утечки по техническим каналам

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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-10*

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 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)
М.Б. Атманских

Методы и средства криптографической защиты информации

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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-9*

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.)**
			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
	Методы и средства криптографической защиты информации	32	0	32	64
1	Введение в теоретико-числовые методы.	2	0	0	2
2	Арифметика больших чисел.	0	0	2	2
3	Теория сравнений.	2	0	0	2
4	Действия в системе вычетов.	0	0	2	2
5	Сравнения первой степени и системы сравнений.	2	0	0	2
6	Решение сравнений и их систем.	0	0	2	2
7	Теория квадратичных вычетов.	2	0	0	2
8	Решение квадратичных сравнений.	0	0	2	2
9	Тесты на простоту.	2	0	0	2
10	Вероятностные тесты на простоту.	0	0	2	2
11	Асимметричные шифры, основанные на проблеме факторизации.	2	0	0	2
12	Асимметричный шифр на проблеме факторизации.	0	0	2	2
13	Мультипликативная группа вычетов.	2	0	0	2
14	Нахождение чисел заданного порядка.	0	0	2	2
15	Асимметричные шифры, основанные на проблеме дискретного логарифмирования.	2	0	0	2
16	Асимметричный шифр, основанный на проблеме дискретного логарифмирования.	0	0	2	2
17	Доказуемо простые числа.	2	0	0	2
18	Доказуемо простые числа.	0	0	2	2
19	Криптоанализ асимметричных криптосистем. Алгоритмы факторизации.	2	0	0	2
20	Алгоритмы факторизации.	0	0	2	2

21	Алгоритмы дискретного логарифмирования.	2	0	0	2
22	Алгоритмы дискретного логарифмирования.	0	0	2	2
23	Цифровые подписи	2	0	0	2
24	Цифровые подписи	0	0	2	2
25	Подписи на эллиптической кривой.	2	0	0	2
26	Эллиптическая кривая.	0	0	2	2
27	Стандарты цифровой подписи на эллиптической кривой.	2	0	0	2
28	Цифровая подпись на эллиптической кривой.	0	0	2	2
29	Криптографические протоколы.	2	0	0	2
30	Разделение секрета.	0	0	2	2
31	Управление ключами.	2	0	0	2
32	Управление ключами.	0	0	2	2
33	Консультация перед экзаменом.	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 дифференцированного зачета (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 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

Методы оценки безопасности компьютерных систем и сетей (пентестинг)

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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:

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.)**
			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
	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 (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 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)
О.А. Нестерова

Основы построения защищенных баз данных

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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-1.3*

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 дифференцированный зачет (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 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)
И.Р. Зулькарнеев

Программно-аппаратные средства защиты информации

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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:

Программно-аппаратные средства защиты информации

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

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
	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 (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 (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 [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)
А.А. Оленников

Научно-проектный (исследовательский) семинар

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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,УК-1,2,3,4,5,9*

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.)**
			8
Общая трудоемкость	**зач. ед.**	4	4
	час	144	144
Из них:			
Часы аудиторной работы (всего):		18	18
Лекции		8	8
Практические занятия		10	10
Лабораторные / практические занятия по подгруппам		0	0
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		126	126
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	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	Подготовка научно-технического отчета	2	0	0	2
6	Презентация и обсуждение плана реализации проекта	0	2	0	2
7	Правила презентации научного исследования	2	0	0	2
8	Презентация и обсуждение промежуточных результатов реализации проекта	0	2	0	2
9	Презентация и обсуждение результатов реализации проекта	0	2	0	2
10	Консультация	0	0	0	0
11	Защита проекта	0	0	0	0
	Итого (ак.часов)	8	10	0	18

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 (8 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)
А.М. Шабалин

Основы построения защищенных компьютерных сетей

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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-1*

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	2	0	0	2
2	Лабораторное занятие 1	0	0	2	2
3	Лекция 2	2	0	0	2
4	Лабораторное занятие 2	0	0	2	2
5	Лекция 3	2	0	0	2
6	Лабораторное занятие 3	0	0	2	2
7	Лекция 4	2	0	0	2
8	Лабораторное занятие 4	0	0	2	2
9	Лекция 5	2	0	0	2
10	Лабораторное занятие 5	0	0	2	2
11	Лекция 6	2	0	0	2
12	Лабораторное занятие 6	0	0	2	2
13	Лекция 7	2	0	0	2
14	Лабораторное занятие 7	0	0	2	2
15	Лекция 8	2	0	0	2
16	Консультация1	0	0	0	0
17	Лабораторное занятие 8	0	0	2	2
18	Лекция 9	2	0	0	2
19	Лабораторное занятие 9	0	0	2	2
20	Лекция 10	2	0	0	2
21	Лабораторное занятие 10	0	0	2	2
22	Лекция 11	2	0	0	2
23	Лабораторное занятие 11	0	0	2	2
24	Лекция 12	2	0	0	2
25	Лабораторное занятие 12	0	0	2	2
26	Лекция 13	2	0	0	2
27	Лабораторное занятие 13	0	0	2	2
28	Лекция 14	2	0	0	2
29	Лабораторное занятие 14	0	0	2	2
30	Лекция 15	2	0	0	2
31	Лабораторное занятие 15	0	0	2	2

32	Лекция 16	2	0	0	2
33	Лабораторное занятие 16	0	0	2	2
34	Консультация 2	0	0	0	0
35	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 экзамен (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 ИМиКН
М.Н. Перевалова
РАЗРАБОТЧИК(И)
И.Р. Зулькарнеев

Проектирование и внедрение систем защиты информации

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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-2,3*

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 дифференцированный зачет (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 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)
А.М. Шабалин

Защита корпоративных сетей

Рабочая программа
для обучающихся по направлению подготовки
10.03.01. Информационная безопасность
Профиль: Безопасность компьютерных систем
(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-2,3*

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
Общая трудоемкость	**зач. ед.**	2	2
	час	72	72
Из них:			
Часы аудиторной работы (всего):		32	32
Лекции		32	32
Практические занятия		0	0
Лабораторные / практические занятия по подгруппам		0	0
Часы внеаудиторной работы, включая консультации, иную контактную работу и самостоятельную работу обучающегося		40	40
Вид промежуточной аттестации (зачет, диф. 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	0	32
	Защита корпоративных сетей	32	0	0	32
1	Лекция 1	2	0	0	2
2	Лекция 2	2	0	0	2
3	Лекция 3	2	0	0	2
4	Лекция 4	2	0	0	2
5	Лекция 5	2	0	0	2
6	Лекция 6	2	0	0	2
7	Лекция 7	2	0	0	2
8	Лекция 8	2	0	0	2
9	Лекция 9	2	0	0	2
10	Лекция 10	2	0	0	2
11	Лекция 11	2	0	0	2
12	Лекция 12	2	0	0	2
13	Лекция 13	2	0	0	2
14	Лекция 14	2	0	0	2
15	Лекция 15	2	0	0	2
16	Лекция 16	2	0	0	2
	Итого (ак.часов)	32	0	0	32

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 (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 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.