МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по УР

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ТЕХНОЛОГИИ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **10.04.01 Информационная безопасность**
Направленность (профиль) / специализация: **Информационная безопасность объектов критической информационной инфраструктуры**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **2**
Семестр: **3**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	3 семестр	Всего	Единицы
Лекционные занятия	16	16	часов
Лабораторные занятия	32	32	часов
Самостоятельная работа	60	60	часов
Общая трудоемкость (включая промежуточную аттестацию)	108	108	часов
	3	3	з.е.

Формы промежуточной аттестация	Семестр
Зачет	3

Томск

1. Общие положения

1.1. Цели дисциплины

1. Подготовить выпускника к деятельности, связанной с выработкой предложений по вопросам построения защищенных каналов передачи данных, разработке предложений по совершенствованию и повышению эффективности комплекса мер защиты каналов передачи данных.

1.2. Задачи дисциплины

1. Изучить принципы построения защищенных каналов передачи данных и управления ими.
2. Обучить студентов использованию программных и аппаратных средств защиты каналов передачи данных.
3. Познакомить студентов с методами проектирования, развертывания и сопровождения защищенных каналов передачи данных.
4. Познакомить студентов с методами обследования и анализа защищенности каналов передачи данных.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль направления подготовки (hard skills – HS).
Индекс дисциплины: Б1.О.2.6.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		

ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	ОПК-2.1. Знает принципы организации и этапы разработки системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Знает принципы построения защищенных каналов передачи данных на объектах критической информационной инфраструктуры и управления ими.
	ОПК-2.2. Знает средства тестирования системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Знает методы анализа защищенности каналов передачи данных на объектах критической информационной инфраструктуры.
	ОПК-2.3. Умеет разрабатывать модели угроз и нарушителей информационной безопасности	Умеет разрабатывать модели угроз и нарушителей для каналов передачи данных на объектах критической информационной инфраструктуры.
	ОПК-2.4. Умеет разрабатывать планы и сценарии тестирования системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Умеет разрабатывать сценарии обследования защищенности каналов передачи данных на объектах критической информационной инфраструктуры.
	ОПК-2.5. Умеет разрабатывать требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Умеет разрабатывать требования к защищенным каналам передачи данных на объектах критической информационной инфраструктуры.
	ОПК-2.6. Умеет разрабатывать и реализовывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Умеет реализовывать защиту каналов передачи данных на объектах критической информационной инфраструктуры в соответствии с сформированными требованиями.
Профессиональные компетенции		
-	-	-

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем

и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		3 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	48	48
Лекционные занятия	16	16
Лабораторные занятия	32	32
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	60	60
Подготовка к зачету	8	8
Написание конспекта самоподготовки	8	8
Подготовка к тестированию	10	10
Подготовка к устному опросу / собеседованию	10	10
Подготовка к лабораторной работе, написание отчета	24	24
Общая трудоемкость (в часах)	108	108
Общая трудоемкость (в з.е.)	3	3

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
3 семестр					
1 Основы построения защищенных каналов передачи данных	6	-	15	21	ОПК-2
2 Технологии обеспечения безопасности в каналах передачи данных	10	32	45	87	ОПК-2
Итого за семестр	16	32	60	108	
Итого	16	32	60	108	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
3 семестр			

1 Основы построения защищенных каналов передачи данных	Определения. Построение каналов передачи данных. сетевые протоколы. Классификация способов построения защищенных каналов передачи информации. Нормативно-правовые основы построения защищенных каналов	2	ОПК-2
	Угрозы каналам связи и передаваемой по ним информации. Уязвимости каналов связи. Классификация атак на каналы связи. Подходы к построению модели угроз и анализу рисков.	2	ОПК-2
	Алгоритмы аутентификации и шифрования. Алгоритмы обмена ключами.	2	ОПК-2
	Итого	6	
2 Технологии обеспечения безопасности в каналах передачи данных	Виртуальные сети ViPNet. Компоненты виртуальной сети ViPNet. Функции координатора. Принципы взаимодействия узлов ViPNet в виртуальной сети. Первоначальные настройки защищенной сети. Механизмы соединений в сети ViPNet. Варианты подключения координаторов к внешней сети. Туннелирование IP-трафика открытых ресурсов. Виртуальные адреса в сети ViPNet. Маршрутизация трафика координаторов с несколькими сетевыми интерфейсами. Туннелирование трафика открытых ресурсов на канальном уровне.	4	ОПК-2
	Построение защищенных каналов на канальном уровне. Протокол PPTP. Протокол L2TP.	2	ОПК-2
	Построение защищенных каналов на сетевом уровне. IPSec. Архитектура IPSec. Заголовок AH. Заголовок ESP. Транспортный режим. Туннельный режим. IKE.	2	ОПК-2
	Построение защищенных каналов на прикладном уровне. Протокол SSL. Протокол TLS. Протокол SSH	2	ОПК-2
	Итого	10	
Итого за семестр		16	
Итого		16	

5.3. Практические занятия (семинары)

Не предусмотрено учебным планом

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
3 семестр			

2 Технологии обеспечения безопасности в каналах передачи данных	Сетевые диагностические утилиты. Сетевые службы.	4	ОПК-2
	Работа с симулятором Cisco Packet Tracer. Виртуальные локальные сети.	4	ОПК-2
	Принципы и функции работы коммутаторов. Маршрутизация.	4	ОПК-2
	Агрегирование каналов.	4	ОПК-2
	Статистическая и динамическая маршрутизация.	4	ОПК-2
	Построение защищенных каналов на канальном уровне. Списки контроля доступа и трансляция адресов.	4	ОПК-2
	Построение защищенных каналов на сетевом уровне. Одноранговые сети.	4	ОПК-2
	Построение защищенных каналов на прикладном уровне. Высокоуровневые службы	4	ОПК-2
	Итого	32	
Итого за семестр		32	
Итого		32	

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
3 семестр				
1 Основы построения защищенных каналов передачи данных	Подготовка к зачету	3	ОПК-2	Зачёт
	Написание конспекта самоподготовки	4	ОПК-2	Конспект самоподготовки
	Подготовка к тестированию	4	ОПК-2	Тестирование
	Подготовка к устному опросу / собеседованию	4	ОПК-2	Устный опрос / собеседование
	Итого	15		

2 Технологии обеспечения безопасности в каналах передачи данных	Подготовка к зачету	5	ОПК-2	Зачёт
	Написание конспекта самоподготовки	4	ОПК-2	Конспект самоподготовки
	Подготовка к тестированию	6	ОПК-2	Тестирование
	Подготовка к устному опросу / собеседованию	6	ОПК-2	Устный опрос / собеседование
	Подготовка к лабораторной работе, написание отчета	24	ОПК-2	Лабораторная работа
	Итого	45		
Итого за семестр		60		
Итого		60		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Лаб. раб.	Сам. раб.	
ОПК-2	+	+	+	Зачёт, Конспект самоподготовки, Устный опрос / собеседование, Лабораторная работа, Тестирование

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
3 семестр				
Зачёт	0	0	30	30
Конспект самоподготовки	3	3	4	10
Устный опрос / собеседование	3	3	4	10
Лабораторная работа	15	15	10	40
Тестирование	0	0	10	10
Итого максимум за период	21	21	58	100
Нарастающим итогом	21	42	100	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 – 100	A (отлично)
4 (хорошо) (зачтено)	85 – 89	B (очень хорошо)
	75 – 84	C (хорошо)
	70 – 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 – 69	
	60 – 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Корячко, В. П. Корпоративные сети [Электронный ресурс]: технологии, протоколы, алгоритмы : монография / В. П. Корячко, Д. А. Перепелкин. — Москва : Горячая линия-Телеком, 2015. — 216 с. — ISBN 978-5-9912-0202-2 [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/111068 .

7.2. Дополнительная литература

1. Основы построения инфокоммуникационных систем и сетей: Учебное пособие / А. В. Пуговкин - 2022. 128 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/9600.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Новохрестов, А. К. Технологии построения защищенных каналов передачи данных: учебно-методическое пособие [Электронный ресурс] / А. К. Новохрестов, А. Ю. Якимук. — Томск: ТУСУР, 2022. — 166 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/9997.

7.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

7.4. Современные профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

8. Материально-техническое и программное обеспечение дисциплины

8.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория безопасности сетей ЭВМ / Лаборатория криптографии в банковском деле: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 804 ауд.

Описание имеющегося оборудования:
- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Усилитель Roxton AA-60M;
- Потолочный громкоговоритель Roxton PA-20T;
- Магнитно-маркерная доска;
- Обучающий стенд локальные компьютерные сети Microtik routerboard - 2 шт.;
- ViPNET УМК "Безопасность сетей";
- Коммутатор Mikrotik CRS125-24G-1S-IN - 6 шт.;
- Анализатор кабельных сетей MI 2016 Multi LAN 350 - 3 шт.;
- Анализатор Wi-Fi сетей NETSCOUT AirCheck G2 - 2 шт.;
- Сервер класса не ниже 4xE7-4809v4/512GBRE16/L9300-8i/5T6000G7;
- Маршрутизатор Cisco 891-K9 - 2 шт.;
- Маршрутизатор Cisco C881-V-K9 - 2 шт.;
- Маршрутизатор Check Point CPAP-SG1200R-NGFW - 2 шт.;

Стенды для изучения проводных и беспроводных компьютерных сетей, включающие:
- абонентские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- межсетевые экраны: ИКС Lite, CISCO ASA 5505, МЭ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- СОВ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- точки доступа: D-link dwl3600ap.

Стенды для изучения средств криптографической защиты информации в банковском деле, включающие:
- абонентские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- средства криптографической защиты информации: программно-аппаратный комплекс шифрования "ФПСУ-IP", программно-аппаратный комплекс шифрования "ФПСУ-IP/Клиент".
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

8.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 209 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

8.4. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися с **нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)

1 Основы построения защищенных каналов передачи данных	ОПК-2	Зачёт	Перечень вопросов для зачета
		Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Тестирование	Примерный перечень тестовых заданий
2 Технологии обеспечения безопасности в каналах передачи данных	ОПК-2	Зачёт	Перечень вопросов для зачета
		Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков

5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

1. По масштабу компьютерные сети подразделяются на
   a) звездообразные, кольцевые, шинные
   b) одноранговые и сети "клиент-сервер"
   c) проводные и беспроводные
   d) локальные и глобальные

2. Задачей какого уровня модели OSI является управление доступом к среде в сетях, построенных на основе разделяемой среды?
   a) прикладного
   b) сетевого
   c) канального
   d) физического

3. Какое минимальное количество уровней протоколов (в терминах модели OSI) должны поддерживать маршрутизаторы сетей с коммутацией пакетов?
   a) 1
   b) 2
   c) 3
   d) 4

4. К транспортному уровню модели OSI относятся протоколы:
   a) IP, RIP, OSPF

b) SSL, TLS
c) SMTP, IMAP, POP3
d) UDP, TCP

5. По какой причине в протоколе RIP расстояние в 16 хопов между сетями полагается недостижимым?
   a) поле, отведенное для хранения значения расстояния, имеет длину 4 двоичных разряда
   b) для получения приемлемого времени сходимости алгоритма
   c) сети, в которых работает RIP, редко бывают большими
   d) таблицы маршрутизации не могут хранить больше 16 записей

6. Что нужно сделать на DHCP сервере чтобы исключить выдачу определенного IP адреса из существующего диапазона?
   a) создать диапазон IP адресов
   b) создать параметр DHCP
   c) создать область DHCP
   d) создать исключение для IP адреса

7. Как называется объект Active Directory, который хранит информацию об учетных записях, общих ресурсах, подразделениях?
   a) сетевой доступ
   b) каталог
   c) папка
   d) домен

8. Какой протокол используется для доступа к службе каталогов AD?
   a) LDAP
   b) ShareDiscovery
   c) ADSL
   d) UDP

9. Компьютер, занимающийся обслуживанием сети, управлением передачей сообщений, и предоставляющий удаленный доступ к своим ресурсам, называется
   a) хабом
   b) сервером
   c) рабочей станцией
   d) хостом

10. Метод передачи данных, при котором данные пересылаются в двух направлениях одновременно, называется …
    a) симплексным
    b) дуплексным
    c) синхронным
    d) полудуплексным

11. Анализ защищенности - это …
    a) выбор обоснованного набора контрмер, позволяющих снизить уровень рисков до приемлемой величины
    b) независимая экспертиза отдельных областей функционирования предприятия
    c) процедура учета действий, выполняемых пользователем на протяжении сеанса доступа
    d) поиск уязвимых мест информационной системы

12. Воздействие на систему с целью создания условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднен.
    a) DoS-атака
    b) несанкционированный доступ

c) незаконное использование привилегий
d) программная закладка

13. Программное средство для удаленной или локальной диагностики различных элементов сети на предмет выявления в них различных уязвимостей.
a) агент безопасности
b) политика безопасности
c) средство делегирования административных полномочий
d) сканер безопасности

14. … - процесс блокировки выявленных вторжений.
a) анализ защищенности
b) обнаружение атак
c) предотвращение атак
d) аудит безопасности

15. В журнале аутентификации обнаружено несколько записей неуспешных попыток войти в систему под учетными записями пользователей. Возможно была попытка подбора паролей. Какое стандартное средство следует использовать для уменьшения риска такого рода атак?
a) использовать систему обнаружения вторжений
b) переименовать учетную запись администратора
c) использовать мультифакторную аутентификацию
d) включить блокировку учетных записей при определенном количестве неуспешных попыток регистрации

16. Политика безопасности требует сокрытия схемы IP-адресации, используемой во внутренней сети. Какая из перечисленных технологий позволит решить поставленную задачу?
a) система обнаружения вторжений
b) персональный межсетевой экран
c) NAT
d) антивирусное программное обеспечение

17. Технология, которая для обнаружения атак использует, например, образец IP-пакета, характерного для какой-нибудь определенной атаки.
a) монитор регистрационных файлов
b) контроль целостности
c) выявление аномальной деятельности
d) анализ сигнатур

18. Согласно классификации ФСТЭК России, межсетевой экран применяемый на логической границе ИС или между логическими границами сегментов ИС, это МЭ …
a) типа А
b) типа Б
c) типа В
d) типа Г

19. Согласно классификации ФСТЭК России системы обнаружения вторжений делятся на
a) уровня узла и уровня сети
b) внешние и внутренние
c) симметричные и асимметричные
d) коммутируемые и некоммутируемые

20. Согласно профилю защиты средства антивирусной защиты типа «Б» устанавливаются на … информационной системы, функционирующей на базе вычислительной сети.
a) рабочие станции пользователей

b) серверы
c) рабочую станцию администратора
d) серверы и рабочие станции

21. Защита ресурсов сети от несанкционированного использования - это
a) охрана оборудования сети
b) защита ядра безопасности
c) контроль доступа
d) защита периметра безопасности

22. Средство защиты, обеспечивающее защищенность информации от угроз нелегитимной передачи данных из защищенного сегмента системы путем анализа и блокирования исходящего трафика
a) межсетевой экран
b) средство антивирусной защиты
c) DLP-система
d) сканер безопасности

23. Средство, решающее задачи консолидации и хранения журналов событий от различных источников, а также имеющее инструменты для анализа событий и разбора инцидентов на основе их корреляции и обработки по правилам – это …
a) DLP-система
b) система обнаружения вторжений
c) SIEM-система
d) сканер безопасности

24. Способ перехвата информации, при котором на машину устанавливается программное средство, собирающее и передающее информацию – это …
a) перехват в разрыв
b) сетевой перехват
c) агентский перехват
d) перехват путем интеграции со сторонними продуктами

25. Программное или аппаратное средство, которое осуществляет мониторинг сети в реальном времени с целью выявления, предотвращения и блокировки вредоносной активности.
a) межсетевой экран
b) система обнаружения вторжений
c) система предотвращения вторжений
d) средство антивирусной защиты

26. К каким методам сбора данных, использующихся при аудите информационной безопасности, относится MaxPatrol?
a) анализ документации
b) предоставление опросных листов
c) использование специализированных программных средств
d) интервьюирование

27. Какой из методов проверки направлен на определение наличия уязвимости по косвенным признакам?
a) активные зондирующие проверки
b) проверка заголовков и активные зондирующие проверки
c) проверка заголовков
d) имитация атак

28. В каком режиме сканирования системы анализа защищенности MaxPatrol можно произвести подбор паролей?

a) Audit
b) Compliance
c) PenTest
d) Pentest и Compliance

29. В каком режиме функционирования IPsec шифруется весь исходный IP-пакет, а затем он вставляется в поле данных нового пакета?
    a) транспортном
    b) туннельном
    c) в обоих режимах
    d) IPsec не использует шифрование

30. Процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности организации в соответствии с определёнными критериями и показателями безопасности – это …
    a) выявление аномальной деятельности
    b) анализ защищённости
    c) аудит информационной безопасности
    d) установка системы защиты

9.1.2. Перечень вопросов для зачета

1. Типовые конфигурации информационных систем. Влияние конфигурации информационной системы на безопасность хранимых, обрабатываемых и передаваемых по сети данных.
2. Угроза. Уязвимость. Атака. Взаимосвязь между этими понятиями.
3. Классификация угроз информационной безопасности вычислительных сетей.
4. Классификация уязвимостей.
5. Классификация атак.
6. Перехват информации в сети. Инструменты. Способы противодействия перехвату.
7. Spoofing. Способы подделки идентификаторов. Способы противодействия spoofing`у.
8. DOS-атаки. Особенности реализации. Способы противодействия DOS-атакам.
9. Универсальные методы обеспечения информационной безопасности компьютеров и компьютерных сетей.
10. Специализированные методы обеспечения информационной безопасности компьютерных сетей.
11. Идентификация и аутентификация. Особенности аутентификации пользователей в компьютерных сетях.
12. Протокол Kerberos. Назначение. Особенности функционирования.
13. Разграничение доступа к информационным ресурсам компьютерных сетей.
14. Криптографическая защита информации в компьютерных сетях. Достоинства и недостатки. Способы преодоления криптографической защиты информации.
15. Электронная подпись. Назначение. Применение для защиты сетевого взаимодействия. Примеры.
16. Сканеры безопасности. Способы выявления уязвимостей в информационных системах.
17. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
18. Системы обнаружения вторжений. Системы предотвращения вторжений. Методики выявления сетевых атак.
19. Сетевые и хостовые системы обнаружения и предотвращения вторжений. Достоинства и недостатки.
20. Межсетевые экраны. Классификация. Варианты размещения межсетевого экрана. Достоинства и недостатки.
21. Демилитаризованная зоны. Назначение. Способы выделения.
22. Классификация межсетевых экранов по уровням защищенности. Показатель защищенности, применяемые для классификации. Применение межсетевых экранов различных классов.
23. Технология VPN (Виртуальные частные сети). Назначение. Достоинства и недостатки.

24. Основные компоненты технологии виртуальных частных сетей (VLAN).
25. Вредоносные программы. Классификация. Каналы распространения. Влияние на информационные системы.
26. Антивирусные средства. Классификация. Методики выявления вредоносного кода.
27. Средства обеспечения информационной безопасности в ОС Windows'2003. Разграничение доступа к данным. Групповая политика. Область действия групповых политик.
28. Основные этапы разработки защищенной компьютерной сети.
29. Проблемы обеспечения безопасности прикладных сервисов (Веб, почта, FTP) и их решения.
30. Физические средства обеспечения информационной безопасности.

9.1.3. Примерный перечень тем для конспектов самоподготовки

1. Принципы взаимодействия узлов ViPNet в виртуальной сети.
2. Варианты подключения координаторов к внешней сети.
3. Протокол PPTP.
4. Архитектура IPSec.
5. Протокол SSL. Протокол TLS.

9.1.4. Примерный перечень вопросов для устного опроса / собеседования

1. Классификация способов построения защищенных каналов передачи информации.
2. Нормативно-правовые основы построения защищенных каналов.
3. Алгоритмы аутентификации и шифрования.
4. Алгоритмы обмена ключами.
5. Виртуальные сети ViPNet. Компоненты виртуальной сети ViPNet.
6. Построение защищенных каналов на канальном уровне.
7. Построение защищенных каналов на сетевом уровне.
8. Построение защищенных каналов на прикладном уровне.

9.1.5. Темы лабораторных работ

1. Сетевые диагностические утилиты. Сетевые службы.
2. Работа с симулятором Cisco Packet Tracer. Виртуальные локальные сети.
3. Принципы и функции работы коммутаторов. Маршрутизация.
4. Агрегирование каналов.
5. Статистическая и динамическая маршрутизация.
6. Построение защищенных каналов на канальном уровне. Списки контроля доступа и трансляция адресов.
7. Построение защищенных каналов на сетевом уровне. Одноранговые сети.
8. Построение защищенных каналов на прикладном уровне. Высокоуровневые службы

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании

изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.2.

Таблица 9.2 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, определяющимися исходя из состояния обучающегося на момент проверки

9.4. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;

– в печатной форме с увеличенным шрифтом;

– в форме электронного документа;

– методом чтения ассистентом задания вслух;

– предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;

– набор ответов на компьютере;

– набор ответов с использованием услуг ассистента;

– представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 1 от «25» 1 2022 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	А.Ю. Якимук	Разработано, 4ffdf265-fb78-4863-b293-f03438cb07cc
Доцент, каф. КИБЭВС	А.К. Новохрестов	Разработано, 1df3f1b6-c21f-4a1c-b6d5-0010ff8a4977