МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра информационной безопасности

ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.04.01 Информационная безопасность
Код и наименование направления подготовки

Организация и технологии защиты государственной тайны
Наименование направленности (профиля)

Уровень высшего образования: *магистратура*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

Технологии защиты информации в компьютерных сетях
Рабочая программа дисциплины
Составитель:
Кандидат технических наук, и.о. зав. кафедрой комплексной защиты информации
Д.А. Митюшин
……..
Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой комплексной защиты информации
Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры КЗИ
№ 8 от 23.03.2023

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – профессиональная подготовка магистрантов, необходимая для освоения методов и технологий защиты информации в компьютерных сетях.
Задачи дисциплины:
дать знания:
– о нормативных правовых актах, нормативными методическими документами ФСБ и ФСТЭК России в области защиты информации ограниченного доступа, циркулирующей в компьютерных сетях;
– о методах и средствах защиты информации в компьютерных сетях;
– о технологии межсетевого экранирования;
– о методах и средствах построения виртуальных частных сетей;
– о методах и средствах аудита защищённости информационных систем.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесённых с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-3 – Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ПК- 3.1 – Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	*Знать:* • правовую основу защиты информации ограниченного доступа • технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами; • методические документы по оценке угроз безопасности информации; • требования по использованию специализированных программно-аппаратных средств при защите информации и проведении аудита информационной безопасности; • методы защиты компьютерных сетей при автоматизации информационных процессов и информатизации предприятий и организаций
	ПК 3.2 -Умеет работать с программным обеспечением с соблюдением	*Уметь:* • применять национальные, межгосударственные и международные стандарты в

	действующих требований по защите информации	области защиты информации, применять действующую законодательную базу в области обеспечения защиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке • выполнять настройку защитных механизмов сетевых программно-аппаратных средств; • настраивать политику безопасности средствами программно-аппаратных комплексов сетевой защиты информации; • организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов
	ПК-3.3 – Владеет организационными мерами по защите информации	*Владеть:* • навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации; • навыками настройки програмно-аппаратных средств защиты информации • навыками настройки политики безопасности средствами программно-аппаратных комплексов сетевой защиты информации.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Технологии защиты информации в компьютерных сетях» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: дисциплина является дисциплиной начального цикла обучения.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Теоретические аспекты безопасности компьютерных систем », «Типовые подсистемы и решения обеспечения информационной безопасности», «Проектно-технологическая практика» и «Преддипломная практика».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 4 з.е., 144 академических часа.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
1	Лекции	32
1	Практические работы	46
	Всего:	78

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 66 академических часов.

3. Содержание дисциплины

Тема 1. Правовая основа защиты информации ограниченного доступа

Основные термины и определения в области защиты информации ограниченного доступа. Основные федеральные законы. Документы Гостехкомиссии (ФСТЭК) России по защите информации ограниченного доступа. Документы ФСБ России по защите информации ограниченного доступа.
Ответственность за преступления в сфере компьютерной информации.

Тема 2. Угрозы безопасности компьютерных сетей

Особенности современных компьютерных сетей (КС). Сети нового поколения. Модели компьютерных сетей. Коммутация и маршрутизация в компьютерных сетях. Адресация в компьютерных сетях.
Угрозы безопасности информации в КС. Утечка информации в КС. Несанкционированный доступ к информации в КС. Уязвимости КС. Виды атак на КС.

Тема 3. Модель угроз и модель нарушителя компьютерных сетей

Разработка модели угроз и модели нарушителя. Руководящие нормативные документы по разработке моделей и определения актуальных угроз.

Тема 4. Межсетевое экранирование

Периметр корпоративной сети. Современные особенности периметра корпоративной сети. Угрозы, связанные с периметром корпоративной сети. Составляющие защиты периметра. Межсетевые экраны их виды. Администрирование межсетевых экранов. Демилитаризованная зона.

Тема 5. Системы обнаружения и предотвращения атак

Системы управления уязвимостями. Анализ содержимого почтового и веб-трафика. Системы обнаружения атак. Классификация систем обнаружения атак.
Системы защиты от утечки информации (DLP-системы).

Тема 6. Основы технологии виртуальных защищённых сетей VPN

Концепция построения виртуальных частных сетей – VPN. Основные понятия и функции сети VPN. Защита информации в процессе её передачи по туннелю VPN. VPN-клиент, VPN-сервер и шлюз безопасности VPN. Реализация механизма VPN. Варианты

построения виртуальных защищённых каналов. Средства обеспечения безопасности VPN. Критерии безопасности данных применительно к задачам VPN. VPN-решения для построения защищённых сетей. Классификация сетей VPN. Критерии классификации. Основные варианты архитектуры VPN. Достоинства применения технологий VPN.

Тема 7. Защита на канальном, сеансовом и сетевом уровнях

Протоколы формирования защищённых каналов на канальном уровне. Протокол PPTP. Структура пакета. Протокол L2TP, его преимущества. Формирование защищённого виртуального канала в протоколе L2TP. Протоколы формирования защищённых каналов на сеансовом уровне. Процедура установления SSL-сессии. Недостатки протоколов SSL и TLS. Протокол SOCKS, его особенности. Схема установления соединения по протоколу SOCKS v5. Защита беспроводных сетей. Протоколы WEP, TKIP, WPA и WPA2.
Защита на канальном, сеансовом и сетевом уровнях. Архитектура средств безопасности IPSec. Компоненты реализаций протокола IPSec имеют следующие. Архитектура стека протоколов IPSec. Защита передаваемых данных с помощью протоколов AH и ESP. Протокол аутентифицирующего заголовка. Применение протокола AH в транспортном и туннельном режимах. Протокол инкапсулирующей защиты, применение протокола ESP в транспортном и туннельном режимах. Алгоритмы аутентификации и шифрования в IPSec. Структура алгоритма HMAC. Протокол управления криптоключами IKE. Задачи, решаемые протоколами IKE. Установление безопасной ассоциации. Базы данных SAD и SPD. Основные схемы применения IPSec.

Тема 8. Защита веб-порталов

Практические аспекты защиты веб-порталов от информационных атак. Типовая архитектура веб-портала. подсистемы антивирусной защиты, контроля целостности, разграничения доступа, обнаружения вторжений, анализа защищённости, криптографической защиты информации, подсистему управления защитой веб-порталов.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	Правовая основа защиты информации ограниченного доступа	Лекция 1. Самостоятельная работа	Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты
2	Тема 2. Угрозы безопасности компьютерных сетей	Лекция 2.1 Лекция 2.2 Самостоятельная работа	Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты
3	Тема 3. Модель угроз и модель нарушителя компьютерных сетей	Лекция 3. Самостоятельная работа	Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты
4	Тема 4. Межсетевое экранирование	Лекция 4. Самостоятельная работа	Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты
5	Тема 5. Системы обнаружения и предотвращения атак	Лекция 5.1 Лекция 5.2 Самостоятельная работа	Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты
6	Тема 6. Основы технологии виртуальных защищённых сетей VPN	Лекция 6.1 Лекция 6.2 Самостоятельная работа	Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты
7	Тема 7. Защита на канальном, сеансовом и сетевом уровнях	Лекция 7.1 Лекция 7.2 Лекция 7.3	Традиционная лекция с использованием презентаций

		Самостоятельная работа	Работа с литературой Консультирование и проверка заданий посредством электронной почты
8	Тема 8. Защита веб-порталов	Лекция 8.1 Лекция 8.2 Самостоятельная работа	Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты
9	Практическое занятие 1. Разработка модели угроз и нарушителя компьютерной сети	Практическое занятие 1. Самостоятельная работа	Выполнение и защита практического задания
10	Практическое занятие 2. Администрирование межсетевых экранов	Практическое занятие 2. Самостоятельная работа	Выполнение и защита практического задания
11	Практическое занятие 3. Создание демилитаризованной зоны	Практическое занятие 3. Самостоятельная работа	Выполнение и защита практического задания
12	Практическое занятие 4. Создание VPN-канала.	Практическое занятие 4. Самостоятельная работа	Выполнение и защита практического задания
13	Практическое занятие 5 (контрольное). Разработка и создание макета защищённой сети организации и филиала	Самостоятельная работа	Выполнение практического задания

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции;

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Максимальное количество баллов	
	За одну работу	**Всего**
Текущий контроль: *- опрос* *- практическое занятие 1* *- практические занятия 2-6*	 *3 балла* *4 балла* *7 баллов*	 *21 балл* *4 балла* *35 баллов*
Промежуточная аттестация – *зачёт с оценкой*		*40 баллов*
Итого за семестр		*100 баллов*

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично/ зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо/ зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
67-50/ D,E	удовлетвори тельно/ зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлетво рительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

№	Вопрос
1.	Понятия «информации», «виды информации» «санкционированный и несанкционированный доступ к информации»
2.	Понятия «персональных данных», виды тайн
3.	Ответственность за преступления в сфере компьютерной информации
4.	Виды сетей
5.	Что такое маршрутизация и метрика?
6.	Что представляет собой физический адрес устройства?
7.	Что представляет собой логический адрес устройства?
8.	Виды атак на компьютерные сети
9.	Уязвимости компьютерных сетей
10.	Разработка модели угроз.
11.	Разработка модели нарушителя.
12.	Межсетевые экраны их виды. Администрирование межсетевых экранов.
13.	Демилитаризованная зона, её понятие и структура
14.	Составляющие защиты периметра.
15.	Особенности периметра современных КС
16.	Реализация механизма VPN

17.	VPN-клиент, VPN-сервер и шлюз безопасности VPN.
18.	Классификация сетей VPN.
19.	Протокол PPTP. Структура пакета.
20.	Процедура установления SSL-сессии.
21.	Защита беспроводных сетей
22.	Архитектура стека протоколов IPSec
23.	Защита передаваемых данных с помощью протоколов AH и ESP
24.	Протокол аутентифицирующего заголовка.
25.	Применение протокола AH в транспортном и туннельном режимах
26.	Протокол инкапсулирующей защиты, применение протокола ESP в транспортном и туннельном режимах.
27.	Протокол управления криптоключами IKE
28.	Задачи, решаемые протоколами IKE
29.	Установление безопасной ассоциации
30.	Базы данных SAD и SPD
31.	Основные схемы применения IPSec
32.	Практические аспекты защиты веб-порталов от информационных атак
33.	Типовая архитектура веб-портала
34.	Подсистемы антивирусной защиты
35.	Подсистемы контроля целостности
36.	Подсистемы разграничения доступа
37.	Подсистемы обнаружения вторжений

Контрольное практическое задание

Студент должен сдать выполненное контрольное задание. Описание задание приведено в п. 9.1

Примерные тестовые задания

1. Что такое виртуальная защищённая сеть VPN?

объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

2. На какие группы делятся сети по признаку «рабочего» уровня модели OSI:

а) VPN канального уровня;
в) VPN сеансового уровня.
г) VPN сетевого уровня;

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

основные

1. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 19.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
2. *Федеральный закон* «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция). Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.

3. *Базовая модель угроз* безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379, свободный. – Загл. с экрана.
4. *Методика оценки угроз безопасности информации*. Методический документ ФСТЭК России от 5 февраля 2021 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g, свободный. – Загл. с экрана.

дополнительные

5. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.
6. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2, свободный. – Загл. с экрана.
7. *Приказ ФСТЭК России* от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=214004&dst=0&rnd=92395C5151F01C02B8725B20C4BBFEB5#034991095371992622 по рабочим дням с 20-00 до 24-00 (время московское), в выходные и праздничные дни в любое время. – Загл. с экрана.
8. *Приказ ФСТЭК России* от 18 февраля 2013 г. № 21. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.. [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=215976&dst=0&rnd=92395C5151F01C02B8725B20C4BBFEB5#08164959407738432 свободный. – Загл. с экрана.

Литература

основная

1. *Щеглов, А. Ю*. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2019. – 309 с. – (Серия : Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. – URL: https://www.biblio-online.ru/book/zaschita-informacii-osnovy-teorii-433715.
2. Запечников, С. В. Основы построения виртуальных частных сетей : учебное пособие / С. В. Запечников, Н. Г. Милославская, А. И. Толстой. – 2-е изд., стер. – Москва : Горячая линия-Телеком, 2011. – 248 с. – ISBN 978-5-9912-0215-2. – Текст :

электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/11834. -- Режим доступа: для авториз. пользователей.
3. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ : учебное пособие / А. Г. Киренберг. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2022. — 120 с. — ISBN 978-5-00137-292-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/257564 (дата обращения: 18.07.2023). — Режим доступа: для авториз. пользователей.

дополнительная

4. *Шаньгин, В. Ф.* Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2012. — 592 с. — ISBN 978-5-94074-637-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/3032 (дата обращения: 18.07.2023). — Режим доступа: для авториз. пользователей.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. *Банк данных угроз безопасности информации*. [Электронный ресурс] / ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» – Режим доступа : URL: https://bdu.fstec.ru/threat, свободный. – Загл. с экрана.
2. *Методика* определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114 -spetsialnye-normativnye-dokumenty/380, свободный. – Загл. с экрана.
3. *Видео уроки* Cisco Packet Tracer. Курс молодого бойца. [Электронный ресурс] : Режим доступа : https://www.youtube.com/playlist?list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9, свободный. – Загл. с экрана.
4. Национальная электронная библиотека (НЭБ) www.rusneb.ru
5. ELibrary.ru Научная электронная библиотека www.elibrary.ru
6. Электронная библиотека Grebennikon.ru www.grebennikon.ru

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное

3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010 или выше	Microsoft	лицензионное
2		Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
4	Cisco Packet Tracer v.7.2	Cisco Systems	условно свободное (необходима регистрация в сетевой академии Cisco)
5	VMware Workstation 15 Player	VMware, Inc	свободное
6	или VirtualBox 6.0	Oracle	свободное
7	Дистрибутивы Linux (например Ubuntu 14)	Oracle	свободное

Средства вычислительной техники, сетевое оборудование, техническое, программное и программно-аппаратные средства защиты информации и средствами контроля защищенности информации.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля подготовки студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических занятий, выдаваемые преподавателем на каждом занятии.

Целью практических занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

Тематика практических занятий соответствует программе дисциплины.

Практическое занятие 1

Тема – ***Разработка модели угроз и нарушителя компьютерной сети***

Задания:

1. Проанализировать угрозы безопасности компьютерной сети организации.
2. Разработать модель угроз безопасности компьютерной сети организации по предложенной форме с учётом нормативных документов ФСТЭК России.
3. Разработать модель нарушителя.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме, нормативные документы ФСТЭК России.
2. Преподавателем выдаётся структура компьютерной сети организации
3. Составить отчёт о выполнении практического задания
4. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС Windows 10 Pro и Microsoft Office 2010.

Практическое занятие 2

Тема – ***Администрирование межсетевых экранов***

Задания:

1. Администрирование межсетевого экрана в ОС Linux и Windows
2. Работа с межсетевым экраном Cisco ASA.
3. Администрирование межсетевых экранов в программе Cisco Packet Tracer.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. На виртуальных машинах установить ОС Linux и Windows (лучше это сделать заранее). Настроить личную учётную запись, выданную преподавателем.
3. Настроить программные межсетевые экраны в ОС. Продемонстрировать их работу.
4. Собрать схему по топологии в Cisco Packet Tracer в индивидуальном адресном пространстве.
5. Обратить внимание на ограничение лицензии при работе с Cisco ASA в Cisco Packet Tracer
6. При работе в чужом адресном пространстве или с чужой учётной записью задание считается невыполненным.
7. Составить отчёт о практическом занятии.
8. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer
2. Развёрнутые виртуальные машиы в количестве 2 шт. на каждом ПК с ОС Linux и Windows

Практическое занятие 3

Тема – ***Создание демилитаризованной зоны***

Задания:

1. Создать демилитаризованную зону с использованием межсетевого экрана Cisco ASA в программе Cisco Packet Tracer.
2. Создать демилитаризованную зону на маршрутизаторе в программе Cisco Packet Tracer.
3. Администрирование межсетевых экранов в программе Cisco Packet Tracer.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Собрать схемы по топологии в Cisco Packet Tracer в индивидуальном адресном пространстве.
3. Обратить внимание на ограничение лицензии при работе с Cisco ASA в Cisco Packet Tracer
4. При работе в чужом адресном пространстве задание считается невыполненным.
5. Составить отчёт о практическом занятии.
6. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:
1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer

Практическое занятие 4
Тема – *Создание VPN-канала*
Задания:
1. Создать VPN-канал между двумя ЛВС поверх канала связи общего пользования.
2. Настроить центр авторизации AAA.

Указания по выполнению заданий:
1. Изучить теоретический материал по теме.
2. Собрать схемы по топологии в Cisco Packet Tracer в индивидуальном адресном пространстве.
3. При работе в чужом адресном пространстве задание считается невыполненным.
4. Составить отчёт о практическом занятии.
5. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:
1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer

Практическое занятие 5
Тема – *Разработка и создание макета защищённой сети организации и филиала*
Данное занятие является контрольным, а задание – контрольным заданием для получения зачёта с оценкой. Для выполнения задания студентам выделяется 18 уч.ч самостоятельной работы и 2 уч.ч для защиты работы.
При полностью функционирующих сетях организации и филиала и работающем защищённом канале студент получает 40 баллов.
Если канал не работает, но работают обе ЛВС и AAA-сервер – 25 баллов. Если при этом не работает AAA-сервер – 15 баллов.
В противном случае контрольная работа считается не выполненной, и студент получается 0 баллов.
За отсутствие на топологии сети «легенды» или недостаточности «легенды» снимается 10 баллов вне зависимости от работоспособности топологии.
Наличие работоспособной топологии является при сдаче зачёта обязательным, отчёта – на усмотрение преподавателя.
Задания:
1. Собрать топологию ЛВС организации и филиала по описанию, предложенном преподавателем.
2. Создать VPN-канал между двумя ЛВС поверх канала связи общего пользования.
3. Настроить центр авторизации AAA.

Указания по выполнению заданий:
1. Изучить теоретический материал по теме.
2. Собрать схемы по топологии в Cisco Packet Tracer в индивидуальном адресном пространстве.
3. При работе в чужом адресном пространстве задание считается невыполненным.
4. Составить отчёт о практическом занятии.
5. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:
1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer

Приложение 1

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Технологии защиты информации в компьютерных сетях» реализуется на факультете Информационных систем и безопасности для студентов 1-го курса, обучающихся по программе магистратуры по направлению подготовки 10.04.01 Информационная безопасность (профиль подготовки – Управление информационной безопасностью) кафедрой комплексной защиты информации.

Цель дисциплины: профессиональная подготовка магистрантов, необходимая для освоения методов и технологий защиты информации в компьютерных сетях.
Задачи:
дать знания:
– о нормативных правовых актах, нормативными методическими документами ФСБ и ФСТЭК России в области защиты информации ограниченного доступа, циркулирующей в компьютерных сетях;
– о методах и средствах защиты информации в компьютерных сетях;
– о технологии межсетевого экранирования;
– о методах и средствах построения виртуальных частных сетей;
– о методах и средствах аудита защищённости информационных систем.

Дисциплина направлена на формирование следующих компетенций:

- ПК-3 – Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

В результате освоения дисциплины обучающийся должен:
Знать:

- правовую основу защиты информации ограниченного доступа
- технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами;
- методические документы по оценке угроз безопасности информации;
- требования по использованию специализированных программно-аппаратных средств при защите информации и проведении аудита информационной безопасности;
- методы защиты компьютерных сетей при автоматизации информационных процессов и информатизации предприятий и организаций

Уметь:

- применять национальные, межгосударственные и международные стандарты в области защиты информации, применять действующую законодательную базу в области обеспечения защиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке
- выполнять настройку защитных механизмов сетевых программно-аппаратных средств;
- настраивать политику безопасности средствами программно-аппаратных комплексов сетевой защиты информации;
- организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов

Владеть:

- навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов,

касающихся защиты информации;
- навыками настройки програмно-аппаратных средств защиты информации
- навыками настройки политики безопасности средствами программно-аппаратных комплексов сетевой защиты информации.

По дисциплине предусмотрена промежуточная аттестация в форме *зачёта с оценкой*.
Общая трудоёмкость освоения дисциплины составляет 4 зачётные единицы.