Аннотация к рабочей программе дисциплины

«Обеспечение информационной безопасности в беспроводных сетях»

Цель преподавания дисциплины

Сформировать основы знаний по принципам построения телекоммуникационных систем беспроводной связи (СБС), а также ознакомление с методами, средствами и системами обеспечения их информационной безопасности.

Задачи изучения дисциплины

– изучения принципов обеспечения безопасности в сетях;
– методов обеспечения безопасности при передаче информации по телекоммуникационной сети;
– определения критериев защищенности сетей;
– механизмов защиты сетей;
– правильного подхода к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

Индикаторы компетенций, формируемые в результате освоения дисциплины

ПК-3 Способен использовать современные методы оценки параметров безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств управления безопасностью, с целью разработки методов устранения выявленных уязвимостей	ПК-3.2 Применяет основные принципы, протоколы и программные криптографические средства обеспечения информационной безопасности сетевых устройств
	ПК-3.3 Применяет стандартные программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа
	ПК-3.4 Пользуется нормативно-технической документацией в области обеспечения информационной безопасности инфокоммуникационных технологий
	ПК-3.5 Осуществляет установку и управление специализированными программными средствами защиты сетевых устройств администрируемой сети от несанкционированного доступа
ПК-4 Способен осуществлять монтаж, наладку, настройку, регулировку, опытную проверку работоспособности, испытания и сдачу в эксплуатацию сооружений, средств и оборудования сетей	ПК-4.3 Использует современные отечественные и зарубежные пакеты программ при решении схемотехнических, системных и сетевых задач, правила и методы монтажа, настройки и регулировки узлов радиотехнических устройств и систем

Разделы дисциплины

1. Сетевая аутентификация
2. Функции межсетевых экранов, профили защиты.
3. Программные и аппаратные средства криптографической защиты
4. Критерии оценки защищенности криптографических модулей
5. Построение VPN
6. Аудит и мониторинг информационной безопасности
7. Критерии выбора сканеров безопасности
8. Методы отражений вторжений

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.О. декана факультета
Фундаментальной и прикладной информатики
(наименование ф-та полностью)

_____М.О. Таныгин
(подпись, инициалы, фамилия)

«30» июня 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Обеспечение информационной безопасности в беспроводных сетях
(наименование дисциплины)

ОПОП ВО 11.03.02Инфокоммуникационные технологии и системы связи
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль) «Системы мобильной связи»
наименование направленности (профиля, специализации)

форма обучения заочная
(очная, очно-заочная, заочная)

Курск – 2022

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки11.03.02 Инфокоммуникационные технологии и системы связи на основании учебного плана ОПОП ВО 11.03.02 Инфокоммуникационные технологии и системы связи, направленность (профиль) «Системы мобильной связи», одобренного Ученым советом университета (протокол № 7 от 25.02.2020 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 11.03.02 Инфокоммуникационные технологии и системы связи, направленность (профиль) «Системы мобильной связи»на заседании кафедры информационной безопасности, протокол № 11 « 30» 06 20 22 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы _____ Кулешова Е.А.
(ученая степень и ученое звание, Ф.И.О.)

Согласовано: на заседании кафедры космического приборостроения и систем связи протокол № 12 « 16 » 06 20 22 г.

Зав. кафедрой _____ АндроновВ.Г.

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 11.03.02 Инфокоммуникационные технологии и системы связи, направленность (профиль) «Системы мобильной связи», одобренного Ученым советом университета протокол № 7 «28» 02 2022 г., на заседании кафедры информационной безопасности протокол №1 от 30.08.2023
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 11.03.02 Инфокоммуникационные технологии и системы связи, направленность (профиль) «Системы мобильной связи», одобренного Ученым советом университета протокол № 7 « 28» 02 2022г., на заседании кафедры ИБ протокол №1 от 29.08.24 .
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель преподавания дисциплины

Целью преподавания дисциплины «Обеспечение информационной безопасности в беспроводных сетях» является формирование у студентов знаний в области обеспечения безопасности беспроводных сетей.

1.2. Задачи изучения дисциплины

– изучения принципов обеспечения безопасности в сетях;

– методов обеспечения безопасности при передаче информации по телекоммуникационной сети;

– определения критериев защищенности сетей;

– механизмов защиты сетей;

– правильного подхода к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК-3	Способен использовать современные методы оценки параметров безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств	ПК-3.2 Применяет основные принципы, протоколы и программные криптографические средства обеспечения информационной безопасности сетевых устройств	***Знать:*** виды угроз и возможные каналы утечки конфиденциальной информации, основные принципы построения криптографических средств, классификацию алгоритмов шифрования и разграничения доступа на уровне локального терминала и в масштабах вычислительной сети. ***Уметь:*** правильно эксплуатировать средства криптографической защиты, снижать вероятность отрицательных

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
	управления безопасностью, с целью разработки методов устранения выявленных уязвимостей.		последствий сетевого взаимодействия за счет применения средств шифрования, применять типовые и собственные средства защиты информации для решения практических задач. ***Владеть:*** навыками применения программных средств защиты информации, разработки программных модулей для криптозащиты пользовательских данных, разработки систем оценки криптостойкости простейших шифров и оценки распределения выходных бит для оценки равномерности распределения данных.
		ПК-3.3 Применяет стандартные программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа	***Знать:*** виды программного и аппаратного обеспечения для защиты сетевых устройств от несанкционированного доступа, особенности применения оборудования в зависимости от масштабов вычислительной сети и наличия прокси-серверов. ***Уметь:*** интегрировать программно-аппаратные средства для повышения уровня информационной безопасности, строить таблицу доверительных узлов сети и исключать доступ подозрительных терминалов путем фильтрации сетевых. ***Владеть:*** навыками применения программных и аппаратных средств защиты информации, интеграции механизмов разграничения доступа на уровне исходного кода и внешней вакцины.
		ПК -3.4 Пользуется нормативно-технической	***Знать:*** нормативно-правовые основы и требования РФ в части обеспечения информационной безопасности при использовании

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		документацией в области обеспечения информационной безопасности инфокоммуникационных технологий	средств учета, обработки и передачи данных. ***Уметь:*** проводить анализ данных, используемых в масштабы вычислительной сети, выделять среди них персональные данные и конфиденциальные сведения. Применять действующие нормативные документы и юридические законы в области защиты информации при оценке защищенности инфокоммуникационных систем. ***Владеть:*** навыками выбора программно-аппаратных средств и телекоммуникационного оборудования, эксплуатации программных средств анализа и управления рисками, навыками разработки или и установки программных продуктов в соответствии с актуальными нормативными требованиями и соблюдением юридических законов в области защиты информации.
		ПК-3.5 Осуществляет установку и управление специализированными программными средствами защиты сетевых устройств администрируемой сети от несанкционированного доступа	**Знать:** устройство межсетевых экранов, технологию оценки состояния защищенности, совместимость программно-аппаратных средств и варианты обеспечения разграничения доступа на уровне операционной системы и прикладных средств. **Уметь:** настраивать режимы работы межсетевых экранов, проводить анализ защищенности локальной вычислительной сети ***Владеть:*** навыками эксплуатации и разработки программно-аппаратных средств обеспечения защиты передаваемых в масштабе вычислительной сети конфиденциальных данных.

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК-4	Способен осуществлять монтаж, наладку, настройку, регулировку, опытную проверку работоспособности, испытания и сдачу в эксплуатацию сооружений, средств и оборудования сетей	ПК 4.3 Использует современные отечественные и зарубежные пакеты программ при решении схемотехнических, системных и сетевых задач, правила и методы монтажа, настройки и регулировки узлов радиотехнических устройств и систем	***Знать:*** особенности современных пакетов программ при решении схемотехнических, системных и сетевых задач по организации взаимодействия удаленных абонентов. ***Уметь:*** настраивать существующие каналы связи, расширять и администрировать локальную вычислительную сети, оптимизировать трафик и обеспечивать уверенный прием в случае использования беспроводного доступа. ***Владеть:*** навыками монтажа, настройки и регулировки узлов радиотехнических устройств и систем.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Безопасность в компьютерных сетях», входит в часть блока 1, формируемую участниками образовательных отношений «Дисциплины (модули») основной профессиональной образовательной программы – программы бакалавриата 11.03.02 Инфокоммуникационные технологии и системы связи, направленность (профиль) «Системы мобильной связи». Дисциплина изучается на 3 курсе.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единицы (з.е.), 108 академических часа.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	8
в том числе:	
лекции	4
лабораторные занятия	4
практические занятия	
Самостоятельная работа обучающихся (всего)	95,9
Контроль (подготовка к экзамену)	
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Сетевая аутентификация	Базовые технологии безопасности. Аутентификация, пароли, авторизация, аудит. Технология защищенного канала. Технологии аутентификации. Сетевая аутентификация на основе многоразового пароля. Аутентификация с использованием одноразового пароля. Аутентификация информации. Понятие подсистемы аутентификации.
2.	Функции межсетевых экранов, профили защиты.	Функции межсетевых экранов. Фильтрация трафика. Выполнение функций посредничества. Дополнительные возможности МЭ. Перечень профилей защиты межсетевых экранов. Понятие межсетевых экранов. Определение типов межсетевых экранов. Типы межсетевых экранов. Фильтрующие маршрутизаторы. Шлюзы сеансового уровня.

		Шлюзы уровня приложений. Типовые схемы подключения межсетевых экранов.
3.	Программные и аппаратные средства криптографической защиты	Классификация угроз, методов и средств защиты информации, определения основных понятий в области криптографии, классические методы шифрования и стандартные криптографические системы, а также программные средства защиты информации (встроенные в ОС и внешние).
4.	Критерии оценки защищенности криптографических модулей	Федеральный стандарт США FIPS 140-2 «Требования безопасности для криптографических модулей». Внешний интерфейс криптографического модуля. Общие требования к криптографическим модулям.
5.	Построение VPN	Предыстория. Сущность VPN. Практическая реализация. Проверка. Понятие туннелирования. Суть туннелирования. Особенность технологии туннелирования. Реализация. Понятие защищенных каналов связей между абонентов виртуальной частной сети. Правила создания этих каналов. Характеристики IP-пакетов. Канальный уровень. PPTP. L2TP. MPLS. Сетевой уровень. IPSec. AH. ESP. IKE. Транспортный уровень. SSL/TLS. Утечка VPN-трафика. Протоколы IPv4 и IPv6. VPN и двойной стек протоколов. Расшифровка VPN-трафика.
6.	Аудит и мониторинг информационной безопасности	Аудит безопасности информационной системы. Проведение аудита безопасности информационных систем. Мониторинг безопасности системы.
7.	Критерии выбора сканеров безопасности	Краткая характеристика. Развертывание и архитектура. Сканирование. Управление результатами сканирования и реагирования. Обновление и поддержка. Дополнительные критерии.
8.	Методы отражений вторжений	Система обнаружения вторжений. Сенсорная подсистема. Подсистема анализа. Хранилище. Консоль управления.

Таблица 4.2 –Содержание дисциплины и её методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (*по неделям семестра*)	Компетенции
		лек, час	№, лаб.	№, пр.			
1	2	3	4	5	6	7	8
1.	Сетевая аутентификация	0,5			У-1-3	С – 1-2	ПК-3
2.	Функции межсетевых экранов, профили защиты.	0,5		1	У-1-3, 4-6 МУ-1-4	С – 3-4 ЗЛР – 3-4	ПК-3,4
3.	Программные и аппаратные средства криптографической защиты	0,5		2	У-1-3, 4-6 МУ-1-4	С – 5-6 ЗЛР– 5-6	ПК-3,4

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (*по неделям семестра*)	Компетенции
		лек, час	№, лаб.	№, пр.			
1	2	3	4	5	6	7	8
4.	Критерии оценки защищенности криптографических модулей	0,5			У-1-3, 4-6	С – 7-8	ПК-3,4
5.	Построение VPN	0,5			У-1-3	С – 9-10	ПК-3,4
6.	Аудит и мониторинг информационной безопасности	0,5		3	У-1-3, 4-6 МУ-1-4	С – 11-12 ЗЛР– 11-12	ПК-3,4
7.	Критерии выбора сканеров безопасности	0,5			У-1-3, 4-6	С – 14-15	ПК-3,4
8.	Методы отражений вторжений	0,5		4	У-1-3 МУ-1-4	С – 16-18 ЗЛР - 16-18	ПК-3,4

С – собеседование, ЗЛР – защита лабораторной работы

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные занятия

Таблица 4.4 – Лабораторные занятия

№	Наименование практической работы	Объем, час.
1.	Настройка межсетевого экрана в операционной системе Windows	1
2.	Фаервол Comodo Firewall	1
3.	Антивирусная программа: Kaspersky Internet Security	1
4.	Анализ защищенности компьютерной сети с помощью программ GFI Languard, Network Security Scanner и XSPIDER	1
Итого		4

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№ раздела (Тема)	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Сетевая аутентификация	1-2 неделя	12
2.	Функции межсетевых экранов, профили защиты.	3-4 неделя	12
3.	Программные и аппаратные средства криптографической защиты	5-6 неделя	12
4.	Критерии оценки защищенности криптографических модулей	7-8 неделя	12

5.	Построение VPN	9-10 неделя	12
6.	Аудит и мониторинг информационной безопасности	11-12 неделя	12
7.	Критерии выбора сканеров безопасности	13-15 неделя	12
8.	Методы отражений вторжений	16-18 неделя	11,9
Итого			95,9

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное «Правилами внутреннего распорядка работников».

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_tele/index.php);

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к зачету;

–методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода не предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся.

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей

образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 7.1 - Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-3. Способен использовать современные методы оценки параметров безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств управления безопасностью, с целью разработки методов устранения выявленных уязвимостей.	Программное обеспечение инфокоммуникаций		Системы коммутации Системы спутникового телерадиовещания
ПК-4. Способен осуществлять монтаж, наладку, настройку, регулировку, опытную проверку работоспособности, испытания и сдачу в эксплуатацию сооружений, средств и оборудования сетей	Теоретические основы систем мобильной связи		Обеспечение информационной безопасности в беспроводных сетях

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
ПК-3, основной.	ПК-3.2 Применяет основные принципы, протоколы и программные криптографические средства обеспечения информационной безопасности сетевых устройств	**Знать**: протоколы и основные методы криптографического преобразования. **Уметь**: шифровать битовую последовательности, заданную в явном виде. **Владеть**: навыками обработки конфиденциальных данных с применением симметричных криптосистем.	**Знать**: протоколы и основные методы криптографического преобразования, каналы утечек, технологию разграничения доступа в масштабах вычислительной сети **Уметь**: применять средства защиты информации для решения практических задач в области информационной безопасности, автоматизировать процесс шифрования. **Владеть**: навыками применения программных средств защиты информации, разработки программных модулей для	**Знать:** принципы построения криптографических средств, классификацию алгоритмов шифрования и разграничения доступа на уровне локального терминала и в масштабах вычислительной сети. **Уметь:** снижать вероятность отрицательных последствий сетевого взаимодействия за счет применения средств шифрования, применять типовые и собственные средства защиты информации для решения практических задач. **Владеть:** навыками разработки систем оценки крипто стойкости

			криптозащиты пользовательских данных.	простейших шифров и оценки распределения выходных бит для оценки равномерности распределения данных.
	ПК-3.3 Применяет стандартные программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа	***Знать:*** разновидности программного и аппаратного обеспечения для защиты сетевых устройств ***Уметь:*** использовать программные средства для повышения уровня информационной безопасности ***Владеть:*** навыками применения программных и средств защиты информации, интеграции	***Знать:*** классификацию программного и аппаратного обеспечения для защиты сетевых устройств от НСД, особенности применения оборудования в зависимости от масштабов вычислительной сети. ***Уметь:*** интегрировать программно-аппаратные средства ЗИ, строить таблицу доверительных узлов сети. ***Владеть:*** навыками применения аппаратных средств защиты информации, интеграции механизмов разграничения доступа на уровне готового продукта.	***Знать:*** особенности применения оборудования в зависимости от масштабов вычислительной сети и наличия прокси-серверов. ***Уметь:*** строить таблицу доверительных узлов сети и исключать доступ подозрительных терминалов путем фильтрации сетевых. ***Владеть:*** навыками применения программных и аппаратных средств защиты информации, интеграции механизмов разграничения доступа на уровне исходного кода и внешней вакцины.
	ПК -3.4 Пользуется нормативно-технической документацией в области обеспечения информационной безопасност	**Знать**: нормативно-правовые акты и законодательства Российской Федерации, регулирующие вопросы защиты информации **Уметь**: определять сферу действия	**Знать**: основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации	**Знать**: нормативно-правовые основы и требования РФ в части обеспечения информационной безопасности при использовании средств учета, обработки и

	и инфокоммуникационных технологий	документа **Владеть:** навыками составления иерархической системы	**Уметь**: определять какая цель в разборе документа **Владеть:** навыками составления интеллектуальной карты	передачи данных. **Уметь**: проводить анализ данных, используемых в масштабы вычислительной сети **Владеть**: навыками выбора программно-аппаратных средств и телекоммуникационного оборудования, эксплуатации программных средств анализа и управления рисками
	ПК-3.5 Осуществляет установку и управление специализированными программными средствами защиты сетевых устройств администрируемой сети от несанкционированного доступа	**Знать**: используемые в работе с ОС программные средства **Уметь**: использовать в работе с ОС программные средства разработки ПО и администрирования **Владеть навыками**: навыками работы с информационно-техническими средствами	**Знать**: инструментальные средства проведения проверок информационных систем **Уметь**: анализ кода программных средств защиты информации **Владеть навыками**: методы проектирования информационных систем с учетом требований информационной безопасности	**Знать:** устройство межсетевых экранов, технологию оценки состояния защищенности, совместимость программно-аппаратных средств и варианты обеспечения разграничения доступа на уровне операционной системы и прикладных средств. **Уметь:** настраивать режимы работы межсетевых экранов, проводить анализ защищенности локальной вычислительной сети ***Владеть:*** навыками эксплуатации и разработки программно-аппаратных

				средств обеспечения защиты передаваемых в масштабе вычислительной
ПК-4, основной	ПК-4.3 Использует современные отечественные и зарубежные пакеты программ при решении схемотехнических, системных и сетевых задач, правила и методы монтажа, настройки и регулировки узлов радиотехнических устройств и систем	***Знать:*** основы работы с программным обеспечением при решении схемотехнических и системных задач связи. ***Уметь:*** настраивать существующие каналы связи. ***Владеть:*** навыками регулировки узлов радиотехнических устройств.	***Знать:*** основы современных пакетов программ при решении и сетевых задач по организации взаимодействия удаленных абонентов. ***Уметь:*** настраивать существующие каналы связи, расширять и администрировать локальную вычислительную сеть ***Владеть:*** навыками монтажа и настройки узлов систем связи.	***Знать:*** особенности современных пакетов программ при решении схемотехнических, системных и сетевых задач по организации сетевого взаимодействия. ***Уметь:*** оптимизировать трафик и обеспечивать уверенный прием в случае использования беспроводного доступа. ***Владеть:*** навыками монтажа, настройки и регулировки узлов радиотехнических устройств и систем.

7.3Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Сетевая аутентификация	ПК-3	Лекция, СРС	Собеседование	1-5	Согласно таблице 7.2
2	Функции межсетевых экранов, профили защиты.	ПК-3	Лекция, СРС, лабораторная работа	Собеседование КВЗЛР №1	1-4 1-4	Согласно таблице 7.2
3	Программные и аппаратные средства криптографической защиты	ПК-3	Лекция, СРС	Собеседование КВЗЛР №2	1-4 1-4	Согласно таблице 7.2
4	Критерии оценки защищенности криптографических модулей	ПК-3	Лекция, СРС	Собеседование	1-4	Согласно таблице 7.2
5	Построение VPN	ПК-3	Лекция, СРС	Собеседование	1-5 1-4	Согласно таблице 7.2
6	Аудит и мониторинг информационной безопасности	ПК-3	Лекция, СРС, лабораторная работа	Собеседование КВЗЛР №3	1-5 1-4	Согласно таблице 7.2
7	Критерии выбора сканеров безопасности	ПК-3	Лекция, СРС	Собеседование	1-4	Согласно таблице 7.2
8	Методы отражений вторжений	ПК-3	Лекция, СРС, лабораторная работа	Собеседование КВЗЛР №4	1-4 1-8	Согласно таблице 7.2

СРС – самостоятельная работа студента, КВЗЛР – контрольные вопросы для защиты лабораторных работ

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы собеседования по разделу (теме) 1. «Сетевая аутентификация»:

1) Что называют сетевой аутентификацией?
2) Что такое авторизация?
3) Перечислите объекты воздействия в информационных системах.
4) Что входит в задачи межсетевых экранов?
5) Что называют контролируемой зоной?

Контрольные вопросы к лабораторной работе №4 «Анализ защищенности компьютерной сети с помощью программ GFI Languard, Network Security Scanner и XSPIDER»:

1) В чем состоит концепция адаптивного управления безопасностью? Перечислите основные компоненты модели адаптивной безопасности.
2) Каков общий принцип работы средств анализа защищенности сетевых протоколов и сервисов?
3) Каков общий принцип работы средств анализа защищенности операционной системы?
4) Каковы методы анализа сетевой информации, используемые в средствах обнаружения сетевых атак?
5) Какова классификация систем обнаружения атак?
6) Перечислите основные компоненты системы обнаружения атак.
7) Каковы положительные и отрицательные стороны систем обнаружения атак на сетевом и операционном уровнях?
8) Дайте общий обзор современных средств обнаружения сетевых атак.

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде бланкового тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

Какая сетевая атака связана с превышением допустимых пределов функционирования сети ?

a. Отказ в обслуживании (DoS –атака).
b. Подслушивание (Sniffing).
c. Атака Man in – the – Middle (человек в середине).
d. Угадывание ключа.

Задание в открытой форме:

1. Сетевое устройство, принимающее поток битов, поступающих из сети, на один из своих портов и передающее этот поток на все остальные порты это …

2. Находятся ли в одной подсети компьютеры с IP-адресами 172.16.2.65 и 172.16.2.94, если у них маска подсети 255.255.255.224….

3. Электронная плата, устанавливаемая в разъем системной платы ком- пьютера и обеспечивающая подключение и прием-передачу данных по линиям компьютерной сети это …

4. Устройство, получающее сетевые пакеты на один из своих портов и передающее их на другой соответствующий порт, определяемый в зависимости от значения адреса сетевого уровня в заголовке пакета, это …

Задание на установление правильной последовательности.

Расположите в правильном порядке уровни модели ISO взаимодействия открытых систем (Open System Interconnect), пронумеровав уровни от нижнего до верхнего от 1 до 7:

1. транспортный
2. физический
3. канальный
4. сетевой
5. представления данных
6. прикладной
7. сеансовый

Задание на установление соответствия:

Установить соответствие названия протокола его назначению

1	FTP	А	Протокол передачи данных
2	SMTP	Б	Протокол передачи файлов
3	TCP/IP	В	Протокол передачи гипертекста
4	HTTP	Г	Протокол передачи почты

Компетентностно-ориентированная задача:

Создать топологию, состоящую из маршрутизатора, к которому подключены 2 компьютера. Между ПК 1 и маршрутизатором подсеть 172.16.0.0, ПК 2 и маршрутизатором подсеть 192.168.0.0. Проверить доступность компьютеров (ПК) с помощью команды ping. Создать Access list, запрещающий прохождений icmp-пакетов из подсети 192.168.0.0. Выполнить команду ping с ПК 1 на ПК 2 и с ПК2 на ПК 1.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016–2018 Обалльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно - рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Лабораторная работа №1	2	Выполнил, доля правильных ответов от 50% до 90%	6	Доля правильных ответов более 90%
Лабораторная работа №2	2	Выполнил, доля правильных ответов от 50% до 90%	6	Доля правильных ответов более 90%
Лабораторная работа №3	2	Выполнил, доля правильных ответов от 50% до 90%	6	Доля правильных ответов более 90%
Лабораторная работа №4	2	Выполнил, доля правильных ответов от 50% до 90%	6	Доля правильных ответов более 90%
Собеседование по темам 1-8	5	Доля правильных ответов от 50% до 90%	12	Доля правильных ответов более 90%
Итого	13		36	
Посещаемость	0		14	
Зачёт	0		60	
Итого	13		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и задача).

Каждый верный ответ оценивается следующим образом:

– задание в закрытой форме –3 балла,

– задание в открытой форме – 3 балла,

– задание на установление правильной последовательности – 3 балла,

– задание на установление соответствия – 3 балла,

– решение компетентностно-ориентированной задачи – 15 баллов.

Максимальное количество баллов за тестирование – 60 баллов.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1) Пролубников, А. В. Сети передачи данных : учебное пособие : в 2 частях / А. В. Пролубников. – Омск : Омский государственный университет им. Ф.М. Достоевского, 2020. – Ч. 1. – 116 с. – URL: https://biblioclub.ru/index.php?page=book&id=614062 . – Режим доступа : по подписке. – Текст : электронный.

2) Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с.– URL: https://biblioclub.ru/index.php?page=book&id=429035. – Режим доступа : по подписке. – Текст : электронный.

3) Васяева, Н. С. Проектирование локальных вычислительных сетей: учебное пособие для курсового проектирования / Н. С. Васяева, Е. С. Васяева. – Йошкар-Ола : Поволжский государственный технологический университет, 2019. – 94 с. – URL: https://biblioclub.ru/index.php?page=book&id=560566. – Режим доступа : по подписке. – Текст : электронный.

8.2 Дополнительная учебная литература

4) Ковган, Н. М. Компьютерные сети : учебное пособие / Н. М. Ковган. – Минск : РИПО, 2019. – 180 с. – URL: https://biblioclub.ru/index.php?page=book&id=599948. – Режим доступа : по подписке. – Текст : электронный.

5) Сети и системы телекоммуникаций: учебное электронное издание / В. А. Погонин, А. А. Третьяков, И. А. Елизаров, В. Н. Назаров. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2018. – 197 с.– URL: https://biblioclub.ru/index.php?page=book&id=570531 . – Режим доступа : по подписке. – Текст : электронный.

6) Кияев, В. Безопасность информационных систем: курс / В. Кияев, О. Граничин. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с. – URL: https://biblioclub.ru/index.php?page=book&id=429032. – Режим доступа : по подписке. – Текст : электронный.

8.3 Перечень методических указаний

1) Настройка межсетевого экрана в операционной системе Windows : методические указания по выполнению лабораторных и практических работ / Юго-Зап. гос. ун-т ; сост. М. О. Таныгин. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2022. - 23 с. - Текст : электронный.

2) Фаервол Comodo Firewall : методические указания по выполнению лабораторных и практических работ / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2022. - 14 с. - Текст : электронный.

3) Антивирусная программа: Kaspersky Internet Security : методические указания по выполнению лабораторных и практических работ / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2022. - 13 с. - Текст : электронный.

4) Анализ защищенности компьютерной сети с помощью программ GFI Languard, Network Security Scanner и XSPIDER : методические указания по выполнению лабораторных и практических работ / Юго-Зап. гос. ун-т ; сост. М. О. Таныгин. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2022. - 12 с. - Текст : электронный.

8.4 Другие учебно-методические материалы

Периодические издания:

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца
2. Журнал «InformationSecurity/Информационная безопасность.»- http://window.edu.ru/
3. Журнал «Проблемы информационной безопасности. Компьютерные системы»- http://window.edu.ru/
4. Журнал «Вестник УрФО. Безопасность в информационной сфере»
5. Журнал «Вопросы защиты информации»
6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»
7. Журнал «Информация и безопасность.»

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://e.lanbook.com - Электронно-библиотечная система «Лань».
2. http://www.iqlib.ru - Электронно-библиотечная система IQLib.
3. http://window.edu.ru -Электронная библиотека «Единое окно доступа к образовательным ресурсам».
4. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».
5. http://www.fsb.ru - Федеральная служба безопасности [официальный сайт].

6. http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт].

7. http://microsoft.com - Корпорация Microsoft[официальный сайт].

8. http://www.consultant.ruКомпания«Консультант Плюс» [официальный сайт].

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины являются лекции и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседованиях). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое

конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

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

MicrosoftOffice 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №К0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут-букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проекторinFocusIN24+

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение

инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14.Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Изме-нённых	Заменённых	Аннулированных	новых			