Аннотация к рабочей программе дисциплины «Мониторинг безопасности телекоммуникационных сетей»

Цель преподавания дисциплины

Целью преподавания дисциплины «Мониторинг безопасности телекоммуникационных сетей» формирование у студентов теоретических знаний в области организации и применения современных технологий и средств мониторинга инфокоммуникационных систем и сетей, практических навыков использования соответствующих программных и технических средств информационных сетей и коммуникационных технологий.

Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

– изучение базовых теоретических принципов построения инфокоммуникационных сетей;

– изучение основных технологий сетей;

– реализовывать правильный подход к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС)

– выработка навыков и умений эксплуатации и мониторинга работоспособности инфокоммуникационных сетей.

Индикаторы компетенций, формируемые в результате освоения дисциплины

ОПК-9.3.1 Использует сканеры безопасности телекоммуникационных систем и сетей.

ОПК-9.3.2 Применяет методы анализа защищенности телекоммуникационных систем и сетей.

ОПК-9.3.3 Проводит настройку средств автоматического реагирования на попытки несанкционированного доступа.

Разделы дисциплины

Введение. Анализ современного состояния сетевой безопасности. Назначение сетевых пакетов и их структура. Анализ сетевого трафика. Программные утилиты для мониторинга сети. Контроль трафика с помощью виртуальных частных сетей. Угрозы информации в беспроводных сетях. Получение информации от сетевых сервисов. Системы мониторинга сетей связи. Системы обнаружения вторжений. Автоматическая валидация уязвимостей с помощью нечетких множеств и нейронных сетей.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
декан факультета
Фундаментальной и прикладной информатики
(наименование ф-та полностью)

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

«27» июня 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Мониторинг безопасности телекоммуникационных сетей
(наименование дисциплины)

ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Управление безопасностью телекоммуникационных систем и сетей»
наименование направленности (профиля, специализации)

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

Курск – 2024

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – специалитет по направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета (протокол № 12 «29» мая 2023 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», на заседании кафедры информационной безопасности протокол №11 «27» июня 2024 г.

Зав. кафедрой Марухленко А.Л.

Разработчик программы
к.т.н. Кулешова Е.А.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета Протокол № « » _____ 20 г., на заседании кафедры информационной безопасности протокол № « » _____ 20 г.

Зав. кафедрой _____

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета Протокол № « » _____ 20 г., на заседании кафедры информационной безопасности протокол № « » _____ 20 г.

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №9 «27» 03 2024 г., на заседании кафедры *информационной безопасности*, протокол №12 от «24» 06 2024 г.

Зав. кафедрой ____________ Марухленко А.Л.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №9 «31» 03 2025 г., на заседании кафедры *информационной безопасности*, протокол № 12 от «24» 06 2025 г.

Зав. кафедрой ____________ Таныгин М.О.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №___«__»______20___г., на заседании кафедры *информационной безопасности*, протокол № ___ от «___»________202__ г.

Зав. кафедрой ____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №___«__»______20___г., на заседании кафедры *информационной безопасности*, протокол № ___ от «___»________202__ г.

Зав. кафедрой ____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №___«__»______20___г., на заседании кафедры *информационной безопасности*, протокол № ___ от «___»________202__ г.

Зав. кафедрой ____

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Целью преподавания дисциплины «Мониторинг безопасности телекоммуникационных сетей» формирование у студентов теоретических знаний в области организации и применения современных технологий и средств мониторинга инфокоммуникационных систем и сетей, практических навыков использования соответствующих программных и технических средств информационных сетей и коммуникационных технологий.

1.2 Задачи дисциплины

В результате изучения дисциплины студенты должны:

– изучение базовых теоретических принципов построения инфокоммуникационных сетей;

– изучение основных технологий сетей;

– реализовывать правильный подход к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС)

– выработка навыков и умений эксплуатации и мониторинга работоспособности инфокоммуникационных сетей.

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*		

ОПК-9.3	Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям	ОПК-9.3.1 Использует сканеры безопасности телекоммуникационных систем и сетей	***Знать:*** Принципы работы сетевых сканеров безопасности. Типы уязвимостей, выявляемых сканерами (CVE, OWASP Top 10, CVSS-метрики). Методы сканирования (активное, пассивное, аутентифицированное, неаутентифицированное). Правовые аспекты проведения сканирования (согласование, ответственность за несанкционированное сканирование). ***Уметь:*** Настраивать и запускать сканирование на различных типах сетей (LAN, WAN, VPN, Wi-Fi). Интерпретировать результаты сканирования (критичность уязвимостей, ложные срабатывания). Формировать отчеты с рекомендациями по устранению уязвимостей. Интегрировать сканеры в систему мониторинга безопасности (SIEM).. ***Владеть (иметь опыт деятельности):*** Навыками работы с популярными сканерами (Nessus, OpenVAS, Nmap). Методиками минимизации ложных срабатываний при сканировании. Практикой безопасного сканирования без нарушения работы сети.
		ОПК-9.3.2 Применяет методы анализа защищенности телекоммуникационных систем и сетей	***Знать:*** Основные методы тестирования на проникновение (Penetration Testing, Red Teaming). Стандарты и методологии оценки защищенности (OSSTMM, PTES, NIST SP 800-115). Техники эксплуатации уязвимостей (MITRE ATT&CK, Metasploit Framework). Особенности анализа защищенности беспроводных, VoIP и IoT-сетей. ***Уметь:*** Проводить ручное и автоматизированное тестирование защищенности. Анализировать логи и трафик (. Выявлять слабые места в конфигурации сетевого оборудования (маршрутизаторы, фаерволы). Оценивать риски на основе результатов тестирования. ***Владеть (иметь опыт деятельности):*** Навыками работы с фреймворками для пентеста. Методами социальной инженерии в контексте оценки защищенности. Практикой составления отчетов по результатам аудита безопасности.
		ОПК-9.3.3 Проводит настройку средств автоматического реагирования на попытки несанкционированного доступа	***Знать:*** Принципы работы систем IDS/IPS. Методы детектирования атак (сигнатурный, аномальный, поведенческий анализ). Протоколы и механизмы автоматического блокирования угроз. Особенности реагирования на DDoS-атаки и APT-угрозы. ***Уметь:*** Настраивать правила обнаружения и блокировки атак в IDS/IPS.

			Интегрировать системы реагирования с SIEM. Анализировать ложные срабатывания и корректировать правила фильтрации. Автоматизировать реакции на инциденты (скрипты, SOAR-платформы). ***Владеть (иметь опыт деятельности):*** Опытом настройки Snort/Suricata и аналогичных систем. Практикой расследования инцидентов с использованием логов IDS/IPS.

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Мониторинг безопасности телекоммуникационных сетей», входит в обязательную часть блока 1 «Дисциплины (модули»») основной профессиональной образовательной программы – программы специалитета 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей». Дисциплина изучается на 5 курсе в 10 семестре.

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 5 зачетных единиц (з.е.), 180 академических часов.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	84
в том числе:	
лекции	42
лабораторные занятия	42
практические занятия	
Самостоятельная работа обучающихся (всего)	67,85
Контроль (подготовка к экзамену)	27
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	1,15

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

4.1 Содержание дисциплины

Таблица 4.1.1 - Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел, (тема) дисциплины	Содержание
1	2	3
1.	Введение. Анализ современного состояния сетевой безопасности	Эволюция угроз. Сдвиги в потребительском восприятии угроз сетевой безопасности. Актуальность технологий предотвращения утечек. Шифрование и многофакторная аутентификация как наиболее эффективные методы защиты. Амплификация. BGP и утечки информации
2.	Назначение сетевых пакетов и их структура	Необходимость упаковки информации. Заголовки пактов. Формат данных в пакте. Методы управления обменом данными. Управление обменом данными в системах с различной топологией. Адресация пакетов.
3.	Анализ сетевого трафика	APM-решения. Признаки комплексного подхода а анализу трафика. Методы анализа сетевого трафика. Парадигмы сетевого мониторинга. Решения в области анализа трафика.
4.	Программные утилиты для мониторинга сети	Назначение, состав, функционал, особенности лицензирования средств мониторинга сети. Состояние рынка средств мониторинга сети. Виды собираемой информации в сетевых мониторах
5.	Контроль трафика с помощью виртуальных частных сетей	Определение виртуальных частных сетей. Принцип действия VPN. Создание туннеля. Процесс инкапсуляции. Туннелирование на уровне 2. Туннелирование IPSec. Поддержка VPN операционными системами. VPN и коммутируемые сети: преимущества и недостатки. Сценарии VPN. VPN удаленного доступа. Виртуальные частные экстрасети. Протоколы туннелирования. Технология PPTP. Технология L2F. Технология L2TP. Режимы тунеллирования. Протоколы шифрования.
6.	Угрозы информации в беспроводных сетях	Особенности беспроводных сетей. Периметр беспроводных сетей. Риски для информации в беспроводных сетях. Уязвимости устройств беспроводной связи. Ошибки конфигурации точек беспроводного доступа. Ошибки конфигурации клиентов беспроводных сетей. Уязвимость криптографических протоколов беспроводных сетей. Утечки информации в беспроводных сетях. Физические особенности среды,

		влияющие на безопасность
7.	Получение информации от сетевых сервисов	Сканирование портов. Получение информации от DNS-сервера. Перебор имен. Перебор обратных записей. Получение информации с использованием SNMP. Получение информации с использованием NetBIOS. Работа с электронной почтой. Анализ баннеров. Получение информации от NTP-сервера.
8.	Системы мониторинга сетей связи	Контроль точек взаимодействия сетей. Управление сетью. Возможности современных систем контроля сетей связи. учёт разговорного трафика. Функциональные возможности систем мониторинга сетей связи. Анализ качества функционирования сети. Анализ разговорной нагрузки по каналам.
9.	Системы обнаружения вторжений. Автоматическая валидация уязвимостей с помощью нечетких множеств и нейронных сетей	Проверка конфигураций и поиск уязвимости ИС. Принципы работы систем обнаружения вторжений. Состав системы обнаружения вторжений. Классификация систем обнаружения вторжений. Размещение компонентов системы обнаружения вторжений в сети. Постановка задачи нечеткой классификации уязвимостей при использовании нейросетей. Принципы работы систем обнаружения вторжений на основе нейросетей.

Таблица 4.1.2 - Содержание дисциплины и ее 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	Введение. Анализ современного состояния сетевой безопасности	4	1		У-1-6 МУ-1-2	УО – 2 ЗЛР - 2	ОПК-9.3
2	Назначение сетевых пакетов и их структура	4	2		У-1-6 МУ-1-2	УО – 4 ЗЛР - 4	ОПК-9.3
3	Анализ сетевого трафика	4	3		У-1-6 МУ-1-2	УО – 6 ЗЛР - 6	ОПК-9.3
4	Программные утилиты для мониторинга сети	4	4		У-1-6 МУ-1-2	УО – 8 ЗЛР - 8	ОПК-9.3
5	Контроль трафика с помощью виртуальных частных сетей	4	5		У-1-6 МУ-1-2	УО –10 ЗЛР - 10	ОПК-9.3
6	Угрозы информации в беспроводных сетях	4	6		У-1-6 МУ-1-2	УО –12 ЗЛР - 12	ОПК-9.3

7	Получение информации от сетевых сервисов	6	7		У-1-6 МУ-1-2	УО –14 ЗЛР - 14	ОПК-9.3
8	Системы мониторинга сетей связи	6	8		У-1-6 МУ-1-2	УО –16 ЗЛР - 16	ОПК-9.3
9	Системы обнаружения вторжений. Автоматическая валидация уязвимостей с помощью нечетких множеств и нейронных сетей	6			У-1-6 МУ-1-2	УО – 18 РСЗ - 18	ОПК-9.3
	Всего	42	-	-			

УО – устный опрос, ЗЛР – защита лабораторной работы, РСЗ – решение ситуационной задачи

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 - Лабораторные работы

№п/п	Наименование лабораторной работы	Объем, час.
1	Средства устранения неисправностей в TCP/IP	4
2	Протокол управления транспортом	4
3	Контроль сетевой активности через VPN	4
4	Беспроводные технологии Bluetooth	6
5	Сетевые утилиты и их использование	6
6	Назначение пакетов и их структура, адресация пакетов	6
7	Анализаторы сетевых протоколов	6
8	Исследование работы телефонной сети на базе АТС Panasonic	6
Итого		42

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Введение. Анализ современного состояния сетевой безопасности	1-2 недели	6

2	Назначение сетевых пакетов и их структура	3-4 недели	6
3	Анализ сетевого трафика	5-6 недели	8
4	Программные утилиты для мониторинга сети	7-8 недели	8
5	Контроль трафика с помощью виртуальных частных сетей	9-10 недели	8
6	Угрозы информации в беспроводных сетях	11-12 недели	8
7	Получение информации от сетевых сервисов	13-14 недели	8
8	Системы мониторинга сетей связи	15-16 недели	8
9	Системы обнаружения вторжений. Автоматическая валидация уязвимостей с помощью нечетких множеств и нейронных сетей	17-18 недели	7,85
Итого			67,85

4. 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 экзамену;

–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 предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования общепрофессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

Таблица 6.1 - Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	2	3	4
1	Автоматическая валидация уязвимостей с помощью нечетких множеств и нейронных сетей	Анализ конкретных ситуаций	8
Итого			8

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения лабораторных занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по направленности (профилю, специализации) программы бакалавриата.

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 профессиональной культуры обуча-

ющихся. Содержание дисциплины способствует правовому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки, высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для природы, человека и общества;

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

– 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
ОПК-9.3 Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты	Мониторинг безопасности телекоммуникационных сетей		Производственная эксплуатационная практика

по выявленным уязвимостям		

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

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап (указывается название этапа изп.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
ОПК-9.3, начальный, основной	ОПК-9.3.1 Использует сканеры безопасности телекоммуникационных систем и сетей ОПК-9.3.2 Применяет методы анализа защищенности телекоммуникационных систем и сетей ОПК-9.3.3 Проводит настройку средств автоматического реагирования на попытки	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ОПК-9.3. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для ОПК-9.3. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ОПК-9.3. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ОПК-9.3.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ОПК-9.3.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ОПК-9.3.

	несанкционированного доступа	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-9.3, не развиты.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-9.3, развиты на элементарном уровне.	***Владеть (или Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-9.3, хорошо развиты.

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	Введение. Анализ современного состояния сетевой безопасности	ОПК-2 ОПК-9	Лекция, СРС, лабораторная работа	Вопросы для устного опроса КВЗЛР	1-10 1-10	Согласно таблице 7.2
2		ОПК-2 ОПК-9	Лекция, СРС, лабораторная работа	Вопросы для устного опроса КВЗЛР	1-10 1-10	Согласно таблице 7.2
3	Назначение сетевых пакетов и их структура	ОПК-2 ОПК-9	Лекция, СРС, лабораторная работа	Вопросы для устного опроса КВЗЛР	1-10 1-10	Согласно таблице 7.2
4		ОПК-2 ОПК-9	Лекция, СРС, лабораторная рабо-	Вопросы для устного опроса КВЗЛР	1-10 1-10	Согласно таблице 7.2

			та			
5	Анализ сетевого трафика	ОПК-2 ОПК-9	Лекция, СРС, лабораторная работа	Вопросы для устного опроса КВЗЛР	1-10 1-10	Согласно таблице 7.2
6		ОПК-2 ОПК-9	Лекция, СРС, лабораторная работа	Вопросы для устного опроса КВЗЛР	1-10 1-10	Согласно таблице 7.2
7	Программные утилиты для мониторинга сети	ОПК-2 ОПК-9	Лекция, СРС, лабораторная работа	Вопросы для устного опроса КВЗЛР	1-10 1-10	Согласно таблице 7.2
8		ОПК-2 ОПК-9	Лекция, СРС, лабораторная работа	Вопросы для устного опроса КВЗЛР	1-10 1-10	Согласно таблице 7.2
9	Контроль трафика с помощью виртуальных частных сетей	ОПК-2 ОПК-9	Лекция, СРС	Вопросы для устного опроса СЗ	1-10 1	Согласно таблице 7.2

СРС – самостоятельная работа студента,

КВЗЛР – контрольные вопросы для защиты лабораторных работ,

СЗ – ситуационная задача.

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 1. «Введение. Анализ современного состояния сетевой безопасности».

1. Как проходила эволюция угроз?

2. Какие происходили сдвиги в потребительском восприятии угроз сетевой безопасности?

3. Какова актуальность технологий предотвращения утечек?

4. Какие существуют наиболее эффективные методы защиты?
5. представляет аутентификация?

Контрольные вопросы для защиты лабораторной работы №1 ««Средства устранения неисправностей в TCP/IP»:

1. Что представляет собой удалённый ресурс? Примеры.
2. Какие способы подключения удалённых ресурсов вам известны?
3. Что такое общий ресурс? Приведите примеры.
4. Как создать общий ресурс?
5. Как подключить удалённый принтер, используя командную строку?

Ситуационные задачи по теме 9 «Системы обнаружения вторжений. Автоматическая валидация уязвимостей с помощью нечетких множеств и нейронных сетей».

Название: «Ложные срабатывания или реальная угроза? Как ИИ помогает анализировать аномалии в корпоративной сети»

Сценарий:

Компания «SecureNet» внедрила систему обнаружения вторжений (IDS) на базе нейронной сети, которая анализирует сетевой трафик и автоматически классифицирует угрозы с применением нечеткой логики для снижения числа ложных срабатываний.

Однако после обновления ПО IDS начала массово блокировать легитимные подключения сотрудников к корпоративному облаку, что парализовало работу отдела разработки. При этом в логах обнаруживаются аномалии, которые система трактует как потенциальные APT-атаки (Advanced Persistent Threat).

Данные для анализа:

1. Логи IDS показывают необычно высокую частоту запросов от нескольких IP-адресов внутри сети к облачному хранилищу.
2. Нейросетевая модель оценивает риск как 87% (высокая угроза), но администраторы подозревают ложное срабатывание.
3. Нечеткий алгоритм валидации учитывает:
   - частоту запросов (высокая/средняя/низкая),
   - время активности (рабочее/нестандартное),
   - тип данных (конфиденциальные/обычные).
4. Сотрудники отдела разработки утверждают, что загружали большие объемы тестовых данных в рамках нового проекта.

Вопросы для обсуждения:

1. Как работает автоматическая валидация угроз с помощью нейронных сетей и нечеткой логики?
   - Какие параметры должна учитывать модель?
   - Почему система могла ошибиться?
2. Какие методы помогут отличить реальную атаку от ложного срабатывания?
   - Нужно ли настраивать весовые коэффициенты в нечеткой системе?
   - Как улучшить обучение нейросети на исторических данных?
3. Какие действия должен предпринять SOC-аналитик?
   - Стоит ли временно отключить блокировку и перевести систему в режим мониторинга?
   - Как настроить правила IDS, чтобы избежать подобных проблем в будущем?
4. Какие риски возникают при излишней автоматизации реагирования?
   - Может ли полностью автономная IDS быть опасной?
   - Где граница между автоматическим блокированием и ручным анализом?

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 экзамена. Экзамен 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:

(1) отказ в обслуживании (DoS –атака)

(2) подслушивание (Sniffing)

(3) атака Man in – the – Middle (человек в середине)

(4) угадывание ключа

Задание в открытой форме:

1) В настоящее время угрозы и вредоносный код разрабатываются с целью – ……

2) Основным средством предотвращения утечек из корпоративных информационных систем являются – ……

3) Что такое неотчуждаемый аутентифицирующий признак - ……..…

Задание на установление правильной последовательности.

1. Установить последовательность команд позволяющие выставить VLAN на интерфейсе.

1) int f1/1.

2) conf t.

3) switchport access vlan 3.

4) write memory.

5) exit, exit.

Задание на установление соответствия:

Установите соответствие между названием и описанием

1	распределенность	А	Срок жизни современных ИБП составляет 10–15 лет, если своевременно выполнять операцию подзарядки батарей
2	управляемость	Б	с любой рабочей станции сети с помощью программы клиента можно наблюдать за состоянием ИБП и получать от него сигналы предупреждения
3	масштабируемость	В	возможность увеличить мощность ИБП
4	долговечность	Г	

Компетентностно-ориентированная задача:

Администратору поручено выбрать сеть, которая бы удовлетворяла следующим требованиям: Количество подсетей — не менее 27. Количество хостов в каждой подсети — не менее 200. Какую маску выберет администратор?

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 О балльно-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
Устный опрос по темам 1-9	6	Доля правильных ответов от 50% до 90%	12	Доля правильных ответов более 90%
Защита лабораторной работы № 1-8	12	Выполнил, доля правильных ответов от 50% до 90%	24	Выполнил,доля правильных ответов более 90%
Решение ситуационной задачи	6	Выполнил, доля правильных ответов от 50% до 90%	12	Выполнил, доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Зачёт	0		36	
Итого	24		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 одна задача).

Каждый верный ответ оценивается следующим образом:
- задание в закрытой форме –2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование –36 баллов.

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

8.1 Основная учебная литература

1. Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие / В. Я. Ищейнов. – Москва ;

Берлин : Директ-Медиа, 2020. – 271 с. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 21.04.2025). – Режим доступа: по подписке. – Текст : электронный.

2. Васильев, К. К. Теория электрической связи : учебное пособие / К. К. Васильев, В. А. Глушков, А. Г. Нестеренко. – Москва ; Вологда : Инфра-Инженерия, 2021. – 468 с. – URL: https://biblioclub.ru/index.php?page=book&id=618556 (дата обращения: 21.04.2025). – Режим доступа: по подписке. – Текст : электронный.

3. Компьютерные сети : учебник / А. Н. Алексахин, С. А. Алексахина, А. В. Батищев [и др.] ; под общ. ред. А. М. Нечаева. – Москва : Университет Синергия, 2023. – 313 с. – URL: https://biblioclub.ru/index.php?page=book&id=699933 (дата обращения: 21.04.2025). – Режим доступа: по подписке. – Текст : электронный.

8.2 Дополнительная учебная литература

4. Козьминых, С. И. Обеспечение комплексной защиты объектов информатизации : учебное пособие / С. И. Козьминых ; Финансовый университет при Правительстве Российской Федерации. – Москва : Юнити-Дана, 2020. – 544 с. – URL: https://biblioclub.ru/index.php?page=book&id=615695 (дата обращения: 21.04.2025). – Режим доступа: по подписке. – Текст : электронный.

5. Пролубников, А. В. Сети передачи данных : учебное пособие : в 2 / А. В. Пролубников. – Омск : Омский государственный университет им. Ф.М. Достоевского (ОмГУ), 2020. – . - URL: https://biblioclub.ru/index.php?page=book&id=614062 (дата обращения: 21.04.2025). – Режим доступа: по подписке. – Текст : электронный. Часть 1. – 116 с.

6. Таныгин, Максим Олегович. Программно-аппаратные системы защиты информации : учебное пособие / М. О. Таныгин ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2012. - 147 с. – Текст : электронный.

8.3 Перечень методических указаний

1. Основы мониторинга безопасности инфокоммуникационных систем и сетей : методические указания по выполнению лабораторных работ 1-8 для студентов, обучающихся по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» по курсу «Основы мониторинга безопасности инфокоммуникационных систем и сетей» / Юго-Зап. гос. ун-

т ; сост. А. Е. Севрюков [и др.]. - Курск : ЮЗГУ, 2019. - 141 с. - Загл. с титул. экрана. - Текст : электронный.

2. Основы мониторинга безопасности инфокоммуникационных систем и сетей : методические указания для самостоятельной работы для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность» / Юго-Зап. гос. ун-т ; сост. М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 10 с. - Текст : электронный.

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

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
3. Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
4. Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru
5. Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
6. База данных "Патенты России"

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины являются лекции, 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, устного опроса, защиты отчетов по лабораторным и 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)

Информационные технологии:

1. Средства для просмотра презентаций;
2. Средства для проведения онлайн-конференций.
3. Электронно-образовательная среда ЮЗГУ

Программное обеспечение:

1. OpenOffice: режим доступа: свободный.
2. Яндекс.Телемост: режим доступа: свободный.

Информационные справочные системы:

1. Научно-информационный портал ВИНИТИ РАН. Режим доступа: свободный.
2. База данных "Патенты России". Режим доступа: свободный.
3. Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: по подписке.
4. Электронная библиотека диссертаций и авторефератов РГБ. Режим доступа: свободный.
5. Электронный каталог Научной библиотеки ЮЗГУ. Режим доступа: свободный.

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

Аудиторные занятия по дисциплине проводятся в учебной аудитории для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенных стандартной учебной мебелью (столы и стулья для обучающихся; стол и стул для преподавателя; доска).

Для организации образовательного процесса применяются технические средства обучения: Проекционный экран на штативе; Мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/1471024Mb/160Gb/ сумка/ проектор inFocus IN24.

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
	Измененных	Заменённых	Аннулированных	новых			