**КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

АНАЛИЗ УЯЗВИМОСТЕЙ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 2 з.е.
в академических часах: 72 ак.ч.

Форма промежуточной аттестации: зачет

2025

Рабочая программа по дисциплине «Анализ уязвимостей компьютерных систем и сетей» по специальности 10.05.01 Компьютерная безопасность, специализации «Разработка защищенного программного обеспечения», составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от «26» ноября 2020 г. № 1459, профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. № 533н, профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. №525н.

Рабочая программа:

обсуждена и рекомендована к утверждению решением кафедры гуманитарных дисциплин и иностранных языков от 21 марта 2025 г., протокол № 7

одобрена Научно-методическим советом Казанского кооперативного института (филиала) от «2» апреля 2025 г., протокол № 3.

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины

Цель дисциплины - «Анализ уязвимостей компьютерных систем и сетей» является обучение передовым методам, моделям, средствам и технологиям обнаружения и анализа уязвимостей, методов и средств их анализа и устранения.

Задачи:

- формирование навыков экспертизы качества и надежности реализаций программных и программно-аппаратных средств обеспечения информационной безопасности;
- формирование навыков анализа программных реализаций на предмет наличия уязвимостей.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Анализ уязвимостей компьютерных систем и сетей» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» основной образовательной программы – программы специалитета по специальности 10.05.01 Компьютерная безопасность специализация «Разработка защищенного программного обеспечения».

Код компетенции	Предшествующие дисциплины (модули), практики	Изучаемые в текущем семестре дисциплины (модули), практики	Последующие дисциплины (модули), практики
ПК-3.4	Паттерны проектирования	**Анализ уязвимостей компьютерных систем и сетей** Физические основы защиты информации	

3. Перечень планируемых результатов обучения по дисциплине

Изучение дисциплины направлено на формирование у обучающихся профессиональных компетенций.

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
ПК-3.4 Способен анализировать уязвимости и угрозы информационной безопасности в компьютерных системах и сетях	ПК-3.4.1Анализирует компьютерную систему с целью определения уровня защищённости и доверия	Знать: основные концепции и стандарты информационной безопасности, типы угроз и уязвимостей компьютерных систем, а также методы их выявления и классификации, методологии и инструменты для оценки уровня защищённости и доверия компьютерных систем. Уметь: идентифицировать компоненты компьютерной системы, подлежащие анализу, проводить анализ рисков для компьютерной системы, выявлять уязвимости и определять потенциальные угрозы, использовать специализированные инструменты и программное обеспечение для сканирования, тестирования и анализа безопасности компьютерных систем. Владеть: навыками применения методов и инструментов анализа защищённости компьютерных систем, навыками выявления, оценки и классификации угроз и уязвимостей компьютерных систем, навыками разработки и реализации рекомендаций по повышению уровня защищённости и доверия компьютерных систем.
	ПК-3.4.2 Демонстрирует умение проводить анализ безопасности компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах	Знать: основные подходы и методики анализа безопасности компонентов программных и программно-аппаратных средств защиты информации, типовые виды атак и сценарии компрометации компонент защитных механизмов, методы верификации и аттестации средств защиты информации, современные средства и технологии мониторинга и аудита безопасности компонент защиты информации. Уметь: проводить детальное исследование функциональности и архитектуры компонент программных и

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
		аппаратных средств защиты информации, выявлять возможные уязвимости и слабые места в компонентах защитной инфраструктуры, оценивать эффективность используемых средств защиты и степень соответствия установленным требованиям и стандартам. Владеть: навыками практической работы с современными инструментами и методами анализа безопасности программных и аппаратных решений, способностью разрабатывать рекомендации по устранению выявленных недостатков и оптимизации настроек существующих средств защиты, методиками документального оформления результатов анализа и оценивания степени риска для автоматизированных систем обработки информации.
	ПК-3.4.3. Формирует предложения по устранению вы- явленных уязвимостей	Знать: основные подходы и принципы устранения уязвимостей программного и аппаратного обеспечения, рекомендации по выбору оптимальных способов нейтрализации выявленных слабых мест, законодательные требования и регламенты, регламентирующие процесс исправления дефектов и повышение уровня защищенности информационных ресурсов. Уметь: анализировать выявленные уязвимости и оценивать их критичность для функционирования системы, определять наиболее эффективные пути ликвидации выявленных проблем и предотвращения возможных инцидентов, составлять аргументированные предложения по модернизации существующей системы защиты. Владеть: навыками разработки конкретных мероприятий по устранению выявленных уязвимостей, умениями формулировать конкретные рекомендации и технические задания на устранение найденных дефектов, наличием опыта управления проектами

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
		по улучшению уровня защиты ИТ-инфраструктуры организаций.

4. Объем дисциплины и виды учебной работы

Объем дисциплины и виды учебной работы в академических часах с выделением объема контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся

очная форма обучения

Вид учебной деятельности		ак.часов	
		Всего	По семестрам
			8
1. Контактная работа обучающихся с преподавателем:		51	51
Аудиторные занятия, часов всего, в том числе:		50	50
• занятия лекционного типа		34	34
• занятия семинарского типа:		16	16
практические занятия		-	-
лабораторные занятия		16	16
в том числе занятия в форме практической подготовки		-	-
Консультации		0,5	0,5
Контактные часы на аттестацию в период экзаменационных сессий		0,5	0,5
2. Самостоятельная работа студентов всего, в том числе		2**1**	2**1**
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		10	20
- выполнение домашних заданий по практическим занятиям		10	20
- подготовка к зачету 1		1	1
Промежуточная аттестация: зачет 1		-	-
ИТОГО:	часов	72	72
общая трудоемкость	зач. ед.	2	2

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Понятие и классификация уязвимостей программного обеспечения

Понятие угрозы и уязвимости и атаки. Классификация и классификаторы уязвимостей. Понятия "уязвимость кода", "уязвимость конфигурации", "уязвимость архитектуры", "организационная уязвимость",

"многофакторная уязвимость". База данных общеизвестных уязвимостей информационной безопасности CVE (англ. Common Vulnerabilities and Exposures).

Обзор банка данных угроз безопасности информации Федеральная служба по техническому и экспортному контролю ФСТЭК России.

Регламент включения информации об уязвимостях программного обеспечения и программно- аппаратных средств в банк данных угроз безопасности информации ФСТЭК России.

Стандарт Common Vulnerability Scoring System (CVSS). ГОСТ Р 56546-2015. ГОСТ Р 58142-2018 МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ

БЕЗОПАСНОСТИ Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045 Классификация уязвимостей информационных систем. Классификация эксплойтов. Анализ стандартов и методик тестирования на проникновение. Уязвимости нулевого дня. Обзор наиболее распространенных и критических уязвимостей.

Тема 2. Актуальные уязвимости современного программного обеспечения. Программные и аппаратные уязвимости.

Аппаратная уязвимость категории утечка по стороннему каналу (Meltdown). Группа аппаратных уязвимостей – Spectre. Уязвимости микропрограмм в постоянных запоминающих устройствах, уязвимости микропрограмм в программируемых логических интегральных схемах, уязвимости базовой системы ввода-вывода, уязвимости ПО контроллеров управления, интерфейсов управления и другие уязвимости. Уязвимости в портативных технических средствах. уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании. уязвимости в средствах защиты информации.

Уязвимости в общесистемном (общем) ПО. Уязвимости в прикладном ПО. Уязвимости в специальном ПО

Тема 3. Уязвимости этапа проектирования программного обеспечения. Методы и инструменты анализа уязвимостей в сфере информационной безопасности.

Методы: экспертный и статистический анализ, анализ документации, сканирование уязвимостей, моделирование атак, тестирование на проникновение, визуализация данных.

Методология тестирования на проникновение: разведка, сканирование и перечисление, получение доступа, повышение привилегии, поддержание доступа, заметание следов, составление отчёта.

Получение отпечатка сбор информации: разведка по открытым источникам, использование общих ресурсов, запрос сведений о регистрации, анализ записей DNS, получение сведений о маршрутизации, автоматизированные инструменты для снятия отпечатков и сбора информации. Методы сканирования и уклонения: сканирование портов,

сетевые сканеры, автоматическое сканирование уязвимостей.

Тема 4. Предотвращение уязвимостей на этапе реализации

Тестирование web-приложений: веб-анализ, межсайтовые сценарии, SQL – иньекция.

Тема 5. Системы обнаружения и предупреждения компьютерных атак

Тестирование беспроводных сетей на проникновение: разведка в беспроводной сети, инструменты тестирования, анализ беспроводного трафика. Мобильное тестирование на проникновение с Kali NetHunter. Инструменты анализа уязвимостей Kali Linux.

5.2. Разделы, темы дисциплины и виды занятий

очная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в часах)			Индикаторы достижения компетенций
		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки (лабораторные работы)	самостоятельная работа	
1	Тема 1. Понятие и классификация уязвимостей программного обеспечения	6	4/4	4	ПК-3.4, ПК-3.4.1, ПК-3.4.2, ПК-3.4.3
2	Тема 2. Уязвимости этапа проектирования программного обеспечения. Методы и инструменты анализа уязвимостей в сфере информационной безопасности.	6	4/4	4	ПК-3.4, ПК-3.4.1, ПК-3.4.2, ПК-3.4.3
3	Тема 3. Уязвимости этапа проектирования программного обеспечения. Методы и инструменты анализа уязвимостей в сфере информационной безопасности.	6	4/4	4	ПК-3.4, ПК-3.4.1, ПК-3.4.2, ПК-3.4.3
4	Тема 4. Предотвращение уязвимостей на этапе реализации	6	2/2	4	ПК-3.4, ПК-3.4.1, ПК-3.4.2, ПК-3.4.3
5	Тема 5. Системы обнаружения и предупреждения компьютерных атак	10	2/2	5	ПК-3.4, ПК-3.4.1, ПК-3.4.2, ПК-3.4.3
	Всего	**34**	**16/16**		

6. Практические занятия

Практические занятия не предусмотрены.

7. Лабораторные работы

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.) Очная форма обучения
1.	Тема 1. Понятие и классификация уязвимостей программного обеспечения	Понятие угрозы и уязвимости и атаки. Классификация и классификаторы уязвимостей. Понятия "уязвимость кода", "уязвимость конфигурации", "уязвимость архитектуры", "организационная уязвимость", "многофакторная уязвимость". База данных общеизвестных уязвимостей информационной безопасности CVE (англ. Common Vulnerabilities and Exposures). Обзор банка данных угроз безопасности информации Федеральная служба по техническому и экспортному контролю ФСТЭК России. Регламент включения информации об уязвимостях программного обеспечения и программно- аппаратных средств в банк данных угроз безопасности информации ФСТЭК России. Стандарт Common Vulnerability Scoring System (CVSS). ГОСТ Р 56546-2015. ГОСТ Р 58142-2018 МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045 Классификация уязвимостей информационных систем. Классификация эксплойтов. Анализ стандартов и методик тестирования на проникновение. Уязвимости нулевого дня. Обзор наиболее распространенных и критических уязвимостей.	4
2.	Тема 2. Актуальные уязвимости современного программного обеспечения. Программные и аппаратные уязвимости.	Аппаратная уязвимость категории утечка по стороннему каналу (Meltdown). Группа аппаратных уязвимостей – Spectre. Уязвимости микропрограмм в постоянных запоминающих устройствах, уязвимости микропрограмм в программируемых логических интегральных схемах, уязвимости базовой системы ввода-вывода, уязвимости ПО контроллеров управления, интерфейсов управления и другие уязвимости. Уязвимости в портативных технических средствах. уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании. уязвимости в средствах защиты информации. зимости в общесистемном (общем) ПО. Уязвимости в прикладном ПО. Уязвимости в специальном ПО	4
3.	Тема 3.	Методы: экспертный и статистический анализ, анализ	4

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.) Очная форма обучения
	Уязвимости этапа проектирования программного обеспечения. Методы и инструменты анализа уязвимостей в сфере информационной безопасности.	документации, сканирование уязвимостей, моделирование атак, тестирование на проникновение, визуализация данных. Методология тестирования на проникновение: разведка, сканирование и перечисление, получение доступа, повышение привилегии, поддержание доступа, заметание следов, составление отчёта. Получение отпечатка сбор информации: разведка по открытым источникам, использование общих ресурсов, запрос сведений о регистрации, анализ записей DNS, получение сведений о маршрутизации, автоматизированные инструменты для снятия отпечатков и сбора информации. Методы сканирования и уклонения: сканирование портов, сетевые сканеры, автоматическое сканирование уязвимостей.	
4.	Тема 4. Предотвращение уязвимостей на этапе реализации	Тестирование web-приложений: веб-анализ, межсайтовые сценарии, SQL – иньекция.	2
5.	Тема 5. Системы обнаружения и предупреждения компьютерных атак	Тестирование беспроводных сетей на проникновение: разведка в беспроводной сети, инструменты тестирования, анализ беспроводного трафика. Мобильное тестирование на проникновение с Kali NetHunter. Инструменты анализа уязвимостей Kali Linux.	2
	Всего		**16**

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Анализ уязвимостей компьютерных систем и сетей» направлена на:

– освоение нормативных правовых актов и учебной литературы, необходимых для освоения дисциплины;

– самостоятельный поиск информации в Интернете и других источниках;

– выполнение домашних заданий по практическим занятиям;

– подготовку к зачету с оценкой.

Краткие рекомендации по выполнению самостоятельной работы:

Успешное усвоение дисциплины предполагает большой, упорный, серьезный, систематический труд студентов. Важнейшая его составная часть – выполнение разных видов самостоятельной работы.

1. **Составление тематического конспекта** на основе изученной

основной и дополнительной учебной литературы. В тематическом конспекте за основу берется содержание темы, вопросы для обсуждения.

Этапы работы.

1.1 Конспектирование делается только после того, как прочитан или усвоен материал для конспектирования.

1.2. Необходимо мысленно или письменно составить план конспекта. По этому плану и будет строиться конспект далее.

1.3. Составление самого конспекта. Можно сказать, что конспект – это расширенные тезисы, дополненные рассуждениями и доказательствами, содержащимися в материалах для конспекта, а также собственными мыслями и положениями составителя конспекта.

Писать конспект рекомендуется четко и разборчиво. В конспекте можно выделять места текста в зависимости от их значимости. Для этого применяются различного размера буквы, подчеркивания, замечания на полях.

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

Примерный перечень заданий для подготовки к тестированию

1. Что такое эксплойт?

(1) компьютерная программа, нейтрализующая уязвимости в программном обеспечении

(2) компьютерная программа, использующая уязвимости в программном обеспечении и применяемая для проведения атаки на вычислительную систему

(3) компьютерная программа, содержащая уязвимости

2. К какому классу относится уязвимость, появившаяся в результате разработки программного обеспечения без учета требований по безопасности информации?

Ответ:

(1) уязвимость архитектуры

(2) уязвимость кода

(3) многофакторная уязвимость

3. К какому классу относится уязвимость, появившаяся в результате выбора, компоновки компонентов программного обеспечения, содержащих уязвимости?

(1) уязвимость архитектуры

(2) уязвимость кода

(3) многофакторная уязвимость

4. Common Vulnerabilities and Exposures (CVE) это...

(1) база данных угроз информационной безопасности

(2) база данных общеизвестных уязвимостей

(3) база данных эксплоитов

(4) база данных наиболее крупных атак на вычислительные системы в мире

5. Что такое CVE Numbering Authority (CNA)?

(1) идентификатор уязвимости

(2) организации, которым разрешено назначать CVE ID уязвимостям в согласованных за ними областях

(3) эксплоит уязвимости

(4) количество уязвимостей одного типа

6. Что такое Primary CAN?

(1) идентификатор уязвимости

(2) организации, которым разрешено назначать CVE ID уязвимостям в согласованных за ними областях

(3) эксплоит уязвимости

(4) организация, курирующая ведение CVE

7. Для чего используется CVSS?

(1) для оценки угроз

(2) для оценки потенциала нарушителя

(3) для оценки уязвимостей

8. Какая версия стандарта CVSS является актуальной?

(1) первая

(2) вторая

(3) третья

(4) четвертая

9. Какие метрики используются для оценки уязвимостей в CVSS?

(1) базовые

(2) стандартные

(3) контекстные (4) временные (5) постоянные

10. В описании угрозы в Банке данных угроз безопасности информации в качестве источника угрозы указаны...

(1) минимальные возможности внешнего или внутреннего нарушителя, необходимые для реализации угрозы

(2) максимальные возможности внешнего или внутреннего нарушителя, необходимые для реализации угрозы

(3) минимальные возможности внутреннего нарушителя, необходимые для реализации угрозы

(4) максимальные возможности внешнего нарушителя, необходимые для реализации угрозы

Примерный перечень заданий для решения стандартных задач

1. Как в CVSS называются характеристики уязвимости, которые не зависят от среды и не меняются со временем? базовые / контекстные/ временные

2. Как в CVSS называются характеристики уязвимости, которые могут измениться со временем? Базовые/ контекстные /временные

4. Как в CVSS называются характеристики уязвимости, которые

зависят от среды? базовые /контекстные /временные

5. Какая базовая метрика CVSS отражает удаленность злоумышленника для использования уязвимости? вектор атаки сложность доступа требуемые привилегии масштаб

6. Какая базовая метрика CVSS показывает, могут ли отличаться уязвимый и атакуемый компоненты? Вектор сложность/ атаки доступа/ требуемые привилегии/ масштаб

7. Какая базовая метрика CVSS отражает сложность реализации атаки? вектор атаки сложность доступа требуемые привилегии масштаб

8. Какая метрика CVSS отражает степень конфиденциальности информации о существовании уязвимости и достоверность известных технических деталей?

Масштаб/ степень достоверности отчета/ уровень исправления зрелость эксплойта

9. Какие метрики CVSS применяются, если аналитик хочет уточнить оценку уязвимости исходя из инфраструктуры и других параметров конкретной организации? базовые контекстные временные

10. Какие метрики CVSS используются опционально? базовые контекстные временные

11. Что содержит вектор уязвимости в CVSS? итоговую численную оценку уязвимости значения метрик для уязвимости перечень метрик для уязвимости без их значений

Примерный перечень заданий для решения прикладных задач

1. Что означает система защиты с полным перекрытием?

(1) для половины (и более) уязвимостей есть устраняющие барьеры

(2) для любой уязвимости есть устраняющий ее барьер

(3) у любой уязвимости есть риск ее реализации

(4) количество уязвимостей меньше, чем количество препятствующих им барьеров

2. При отсутствии в системе барьеров, «перекрывающих» выявленные уязвимости, степень сопротивляемости механизма защиты принимается равной...

(1) 0

(2) 1

3. Защищенность системы защиты определяется как величина...

(1) обратная суммарному количеству рисков

(2) обратная остаточному риску

(3) обратная уязвимости

(4) равная сумме всех уязвимостей

3. Что из нижеперечисленного относится к оперативным методам повышения безопасности?

(1) систематическое тестирование

(2) предотвращение ошибок в CASE-технологиях

(3) обязательная сертификация

(4) программная избыточность

4. Что из нижеперечисленного относится к мерам предотвращения угроз безопасности?

(1) систематическое тестирование

(2) предотвращение ошибок в CASE-технологиях

(3) обязательная сертификация

(4) программная избыточность

5. Выделите внешние по отношению к объекту уязвимости дестабилизирующие факторы и угрозы безопасности:

(1) ошибки персонала при эксплуатации

(2) ошибки программирования

(3) сбой и отказы аппаратуры ЭВМ

(4) ошибки алгоритмизации задач

6. Выделите внутренние по отношению к объекту уязвимости дестабилизирующие факторы и угрозы безопасности:

(1) ошибки персонала при эксплуатации

(2) ошибки программирования

(3) сбой и отказы аппаратуры ЭВМ

(4) ошибки алгоритмизации задач

7. На каких принципах должна строиться архитектура ИС?

(1) проектирование на принципе закрытых систем

(2) проектирование на принципе открытых систем

(3) усиление самого сильного звена

(4) усиление самого слабого звена (5) эшелонирование обороны

8. Злоумышленники часто используют для атак:

(1) уязвимости Web-серверов

(2) уязвимости X-Window

(3) уязвимости почтовых серверов

10. Nessus - это: Ответ:

(1) сканер портов

(2) сканер уязвимостей без встроенного сканера портов

(3) сканер уязвимостей со встроенным сканером портов

Перечень вопросов, которые выносятся на зачет

Вопросы к зачету

1. Основные понятия информационной безопасности.

2. Основные составляющие. Доступность, целостность и конфиденциальность информации.

3. Доктрина информационной безопасности РФ.

4. Классификация защищаемой информации по степени важности и ценности.

5. Основные определения и критерии классификации угроз.

6. Законодательный уровень информационной безопасности.

7. Административный уровень информационной безопасности.

8. Содержание политики безопасности. Программа безопасности.

9. Управление рисками. Основные понятия. Подготовительный этап управления рисками.

10. Управление рисками. Основные этапы управления рисками.

11. Методы и модели анализа угроз.

12. Поддержание работоспособности. Реагирование на нарушения режима безопасности.

13. Основные программно-технические меры.

14. Архитектурная безопасность.

15. Идентификация и аутентификация, управление доступом.

16. Мониторинг и аудит.

17. Шифрование, контроль целостности.

18. Экранирование, анализ защищенности.

19. Классификация межсетевых экранов.

20. Основные причины возможности проведения атаки типа Инъекция.

21. Алгоритм поведения атаки типа Иньекиия на скрипт-коды.

22. Алгоритм проведения атаки типа SQL-инъекция

23. Классификация XSS атак.

24. Отличия между хранимой и временной XSS атаками.

25. Понятия и сущность Flood-атаки.

26. Различия между DoS и DDoS атаками.

27. Методы проведения DNS-атак.

28. Методы проведения атаки BruteForce.

29. Условия успешного проведения атак типа DoS/DDoS/Flood. 30 Причины актуальности сетевых удаленных атак.

31. Сущность активного сканирования атакуемого сетевого ресурса.

32. Сущность пассивного сканирования атакуемого сетевого ресурса.

33. Методы анализа атакуемого узла

10. Оценивание результатов обучения и уровня сформированности компетенций

Оценивание результатов обучения по дисциплине и уровня сформированности компетенций (части компетенции) осуществляется в рамках текущего контроля успеваемости и промежуточной аттестации в соответствии с оценочными материалами.

11. Учебно-методическое обеспечение дисциплины

Основная литература:

1. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие/ Ю. Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557

2. Гисин, В. Б. Криптография и распределенные реестры : учебное

пособие : [16+] / В. Б. Гисин ; Финансовый университет при Правительстве Российской Федерации. – Москва : Прометей, 2022. – 186 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700941 (дата обращения: 01.03.2025). – Библиогр. в кн. – ISBN 978-5-00172-257-1. – Текст : электронный.

3. Информационная безопасность. Практические аспекты : учебник для вузов / Л. Х. Сафиуллина, А. Р. Касимова, Я. С. Рябов [и др.]. — Санкт-Петербург : Интермедия, 2021.

— 240 с. — ISBN 978-5- 4383-0205-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/103997.html

4. Основы защиты информации в современных информационных системах : учебное пособие / Н. Ю. Бабанов, А. А. Евстифеев, А. П. Мартынов [и др.]. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2022. — 175 с. — ISBN 978-5-9515-0491-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/132622.html

5. Методы теории оптимального управления в задачах защиты компьютерных систем от вирусных атак : учебное пособие / Н. А. Семыкина. — Тверь : Тверской государственный университет, 2020. — 100 с. — ISBN 978-5-7609-1574-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART :[сайт]. — URL: https://www.iprbookshop.ru/111573.html

Дополнительная литература:

1. Скулкин, О. Шифровальщики : как реагировать на атаки с использованием программ- вымогателей : [16+] / О. Скулкин ; науч. ред. А. Алексеев ; ред. К. Ахметов ; пер. с англ. А. Власюк. – Москва : Альпина Паблишер, 2023. – 205 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=707831 (дата обращения: 01.03.2025). – ISBN 978-5-206-00080-1. – Текст : электронный.

2. Лапонина, О. Р. Протоколы безопасного сетевого взаимодействия [Электронный ресурс]: курс/ О. Р. Лапонина. - 2-е изд., исправ. - Москва: ИНТУИТ, 2016. - 462 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=429094

Электронные библиотечные системы (ЭБС) и электронные образовательные ресурсы

1. Электронно-библиотечная система ZNANIUM https:// www.znanium.com
2. Универсальная справочно-информационная полнотекстовая база данных периодических изданий «East View» (ИВИС) https://dlib.eastview.com/
3. Электронно-библиотечная система «BOOK.ru» www.book.ru
4. Электронно-библиотечная система «IPRbooks»

http://www.iprbookshop.ru/

5. ЭБС «Национальный цифровой ресурс «Руконт» https://lib.rucont.ru/search

6. Образовательная платформа ЮРАЙТ http://www.urait.ru

Электронный каталог Университета – Автоматизированная информационная библиотечная система (АИБС «МегаПро»)

12. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

Лицензионное программное обеспечение, в том числе отечественного производства:

– DsktpEdu ALNG LicSARk OLV F1 1Y Acdmc Ent (MS Windows) (подписка на ПО).

Свободно распространяемое программное обеспечение, в том числе отечественного производства:

– 7-Zip (свободный файловый архиватор с высокой степенью сжатия данных) (отечественное ПО).

– FastStone Image Viewer (программа для просмотра изображений в Microsoft Windows (лицензия бесплатного программного обеспечения)).

– Foxit Reader (Бесплатное прикладное программное обеспечение для просмотра электронных документов в стандарте PDF (лицензия бесплатного программного обеспечения)).

– Indigo (система программ для создания и проведения компьютерного тестирования знаний).

– Google Crome, ЯндексБраузер (браузер).

– Adobe Acrobat Reader DC (• ПО для просмотра, печати и комментирования документов в формате PDF)

– Visual Studio Code (интегрированная среда разработки программного обеспечения)

Профессиональные базы данных не используются.

Информационные справочные системы:

– СПС КонсультантПлюс. Компьютерная справочная правовая система, широко используется учеными, студентами и преподавателями (подписка на ПО)

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной

13. Материально–техническое обеспечение дисциплины

Образовательный процесс обеспечен учебными аудиториями для проведения учебных занятий, а именно для проведения занятий лекционного типа, лабораторных занятий, групповых и индивидуальных консультаций,

текущего контроля и промежуточной аттестации, помещениями для самостоятельной работы студентов.

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Рабочее место преподавателя (стол, стул), рабочие места обучающихся, доска для написания мелом, кафедра.

Технические средства обучения: персональный компьютер-1, мультимедийное оборудование (проектор, проекционный экран) - 1

Учебная аудитория для проведения лабораторных занятий. Учебная аудитория для проведения лабораторных занятий. Лаборатория сетей и систем передачи информации, безопасности компьютерных сетей

Рабочее место преподавателя (стол, стул), рабочие места обучающихся:

Технические средства обучения: персональный компьютер с подключением к сети «Интернет» - - 15, сетевое оборудование; стенды; коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, средства обнаружения компьютерных атак, средства анализа защищенности компьютерных сетей

Учебная аудитория для проведения лабораторных занятий. Аудитория информационных технологий

Рабочее место преподавателя (стол, стул), рабочие места обучающихся:

Технические средства обучения:

персональный компьютер с подключением к сети «Интернет» - 15, сетевое оборудование.

Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду института.

Рабочие места обучающихся.

Технические средства обучения: персональный компьютер - 13.

Учебные аудитории соответствуют действующим противопожарным правилам и нормам, укомплектованы учебной мебелью.

Обновление рабочей программы дисциплины (модуля)

Наименование раздела рабочей программы, в который внесены изменения

(измененное содержание раздела)

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____