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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОПЕРАЦИИ И АТАКИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ СЕТЯХ

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 «Операции и атаки в компьютерных системах сетях» 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

Целью преподавания и изучения дисциплины «Операции и атаки в компьютерных системах сетях» является формирование у студентов способности оценивать угрозы информационной безопасности и разрабатывать архитектурные и функциональные спецификации создаваемых систем и средств по ее защите, а также разрабатывать методы реализации и тестирования таких систем.

Задачи: студент должен знать основные понятия, методы, алгоритмы и технологии защиты информации; уметь применять теории и методы по обеспечению компьютерной безопасности; владеть технологиями реализации систем такой защиты.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Операции и атаки в компьютерных системах сетях» 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-3.6.	Коллективная разработка приложений Администрирование в Linux Коллективная разработка приложений Администрирование информационных сетей	**Операции и атаки в компьютерных системах сетях**	Компьютерные преступления в компьютерных системах и сетях

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-3.6 Способен участвовать в работах по противодействию информационным атакам и операциям, реализуемым в компьютерных системах и сетях	ПК-3.6.1Выполняет анализ защищенности компьютерных систем и сетей с использованием сканеров безопасности.	Знать: содержание информационной безопасности и ее место в системе национальной безопасности, основные угрозы и методы защиты от них, системные методологии, международные и профессиональные стандарты в области информационной безопасности.. 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: уверенное владение Windows, Linux и другими ОС в контексте настройки и анализа систем безопасности, уверенное владение инструментами, такими как Metasploit, Burp Suite и другими для проведения пентестов, понимание принципов шифрования и защиты данных в процессе передачи и хранения.
	ПК-3.6.2 Реализует анализ защищенности сетевых сервисов автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей	Знания: Основы информационной безопасности и защиты сетевых сервисов. Типы атак на сетевые сервисы (DDoS, SQL-инъекции, XSS и др.). Принципы работы систем обнаружения и предотвращения вторжений (IDS/IPS). Нормативные документы и стандарты по безопасности информации. Умеет: использовать углубленные теоретические и практические знания в области информационной безопасности. Владение: Уверенное использование средств мониторинга и анализа трафика (Wireshark, Snort). Настройка и администрирование брандмауэров и прокси-серверов. Владение языками программирования для автоматизации процессов (Python, Bash). Опыт работы с системами управления инцидентами безопасности (SIEM).
	ПК-3.6.3.Структурирует аналитическую	Знать:Основы анализа данных и информационной безопасности.

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
	информацию для составления отчётов по результатам проверок качества противодействия информационным атакам и операциям, реализуемым в компьютерных системах и сетях	Методы оценки качества систем защиты от информационных атак. Стандарты и шаблоны для составления отчетов по безопасности (например, NIST, ISO). Типы информационных атак и их влияние на компьютерные системы и сети. Уметь: Сбор и анализ данных о результатах проверок качества систем безопасности. Структурирование информации для создания понятных и информативных отчетов. Выявление ключевых показателей эффективности (KPI) в области безопасности. Формулирование рекомендаций по улучшению качества противодействия атакам. Владеть: навыками использования технологий обеспечивающих создание безопасных программных решений.

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
			9
1. Контактная работа обучающихся с преподавателем:		35	35
Аудиторные занятия, часов всего, в том числе:		34	34
• занятия лекционного типа		16	16
• занятия семинарского типа:		18	18
практические занятия		18	18
лабораторные занятия			
в том числе занятия в форме практической подготовки		-	-
Иная контактная работа:		0,5	0.5
Контроль самостоятельной работы (КСР)		2	2
Промежуточная аттестация (ИКР)			
2. Самостоятельная работа студентов всего, в том числе		37	37
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		15	15
- выполнение домашних заданий по практическим занятиям		15	15
- подготовка к зачету		5,8	5,8
Промежуточная аттестация: зачет		-	-
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. Содержание понятия безопасность и его структура. Проектирование алгоритмов поддержки информационной безопасности.

Виды безопасности и связи между ними. Анализ угроз информационной безопасности. Правовая поддержка организации информационной безопасности. Смысл компьютерной безопасности, ее основные требования. Основные понятия актуализации компьютерной безопасности.

Тема 2. Стандарты информационной безопасности.

Организация вычислений на графе. Кодирующие и декодирующие преобразования. Алгоритмы защиты данных, основанные на комбинаторике и теории чисел.

Тема 3. Сценарий Идентификация- Аутентификация- Авторизация и варианты реализации.

Критерии безопасности компьютерных систем (Оранжевая книга). ISO/IEC 17799:2002 “Управление информационной безопасностью”. ISO 15408 “Общие критерии безопасности информационных технологий” “CommonCriteria”ОК). Российские стандарты в области информационной безопасности.

Тема 4. Модели управления доступом к информаци
и. Модели поддержан ия целостност и информации

Подходы к идентификации и аутентификации. Понятие полномочий и ролей, их виды. Реализация сценария идентификации- аутентификации-авторизации в операционных системах Windows и Unix.

Тема 5. Аудит вычислительной системы и архивация. Анализ уязвимости системы. DLP- системы.Системы обнаружения вторжений

Монитор безопасности. Основные политики доступа. Модель HRU. Модель Белла-ЛаПадулы. Модель МакЛина. Модель Take-Grant. Модель Китайская стена.

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 (лабораторная работа)	самос-тоятельная работа	
1	Тема 1. Содержание понятия безопасность и его структура. Проектирование алгоритмов поддержки информационной безопасности.	3	3	8	ПК-3.6.1 ПК-3.6.2, ПК-3.6.3,
2	Тема 2. Стандарты информационной безопасности.	3	3	8	ПК-3.6.1 ПК-3.6.2, ПК-3.6.3,
3	Тема 3. Сценарий Идентификация-Аутентификация-Авторизация и варианты реализации.	3	3	8	ПК-3.6.1 ПК-3.6.2, ПК-3.6.3,
4	Тема 4. Модели управления доступом к информаци и. Модели поддержан ия целостност и информаци	3	3	8	ПК-3.6.1 ПК-3.6.2, ПК-3.6.3,
5	Тема 5. Аудит вычислительной системы и архивация. Анализ уязвимости системы. DLP-системы. Системы обнаружения вторжений	4	6	5	ПК-3.6.1 ПК-3.6.2, ПК-3.6.3,
	Всего	**16**	**18**	**37**	

6. Лабораторные работы

Лабораторные работы не предусмотрены.

7. Практические занятия

№ п/п	Наименование раздела, темы дисциплины	Содержание практических занятий	Объем (час.)
			Очная форма обучения
1.	Тема1. Проектирование алгоритмов	Поля объектов и проблема защиты информации	4

№ п/п	Наименование раздела, темы дисциплины	Содержание практических занятий	Объем (час.)
			Очная форма обучения
	поддержки информационной безопасности.		
2.	Тема 2. Стандарты информационной безопасности.	Поля объектов и проблема защиты информации. Основные свойства и параметры волн различной природы и различных частотных диапазонов при распространении в идеальных и реальных средах, способы и устройства возбуждения и приема волн	4
3.	Тема 3. Сценарий Идентификация-Аутентификация-Авторизация и варианты реализации.	Электрические, магнитные и электромагнитные поля объектов. Электромагнитные волны, их характеристики, свойства и особенности распространения в различных средах	4
4.	Тема 4. Модели управления доступом к информации. Модели поддержания целостности информации.	Модели управления доступом к информации. Модели поддержания целостности информации	6
	Всего		**18**

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Базы данных» 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.

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

Зачетно-экзаменационные материалыдля промежуточной аттестации (зачет с оценкой)

1.Классификация информационных угроз.
2.Основные качества защищенной информации в ИС.
3.В чем смысл политики безопасности.
4.Что такое несанкционированный доступ (НСД) и их виды.
5.Что такое уязвимость, атака, структура атаки и возможные виды атак.
6.Виды моделей доступа к данным, их характеристика.
7.Назначение стандартов информационной безопасности. Структура стандартов.
8.Что такое сниффинг, спуффинги hijacking.
9.Что такое DOS-атака, DDOS-атака ,SYN-атака.
10.Является ли алгоритмически разрешимым свойство быть безопасной системой в модели HRU.
11.Какого вида данные обязаны находиться в открытом доступе.
12.Назовите уровни секретности данных, которые регламентирует закон РФ “О государственной тайне”.
13.Классификация информационных угроз.
14.Основные качества защищенной информации в ИС.
15.В чем смысл политики безопасности.
16.Что такое несанкционированный доступ (НСД) и их виды.
17.Что такое уязвимость, атака, структура атаки и возможные виды атак.
18.Виды моделей доступа к данным, их характеристика.
19.Назначение стандартов информационной безопасности. Структура стандартов.
20.Что такое сниффинг, спуффинги hijacking.

21.Что такое DOS-атака, DDOS-атака ,SYN-атака.
22.Является ли алгоритмически разрешимым свойство быть безопасной системой в модели HRU.
23.Какого вида данные обязаны находиться в открытом доступе. Назовите уровни секретности данных, которые регламентирует закон РФ“О государственной тайне”.
24.Механизм идентификации, аутентификации и авторизации в ОС Unix.
25.Механизм идентификации, аутентификации и авторизации в ОС Windows.
26.Биометрические методы аутентификации
27.Механизм одноразовых паролей
28.Протокол аутентификации Kerberos
29.Основные положения дискреционной модели полномочий HRU
30.Основные положения мандатной модели полномочий Белла-ЛаПадулы
31.Модель полномочий Мак-Лина.
32.Классификация зловредного программного обеспечения.
33.Особенности полиморфного вируса и руткита.
34.Основные положения VPN-сети.
35.Назначение методов социальной инженерии и их формы.
36.Назначение и формы аудита в ОС Windows.
37.Назначение и механизм сетевого экрана.
38.Характеристика средств информационной безопасности в рамках стека протоколов ISO OSI.
39.Структура угроз информационной безопасности.
40.Содержание основных понятий ИБ: «защищенность данных», «уязвимость»,
«атака», «злоумышленник» и др. Их отражение в стандартах ИБ.

Код оцениваемой компетенции: ПК-3.4

Образцы билетов

Билет №1
1.Правила NRU и NWD . Области использования этих правил.
2.Характеристика схемы симметричного шифрования. Достоинства и недостатки этой схемы.
3.Сколько времени необходимо на расшифровку ключа алгоритма DES на компьютере с быстродействием 1000 млрд. операций в секунду если один ключ расшифровывается за 10 операций.

Билет №2
1.Основные компоненты модели Take-Grant. Понятие графа доступов и его пример.
2.Протокол аутентификации Kerberos.

3.Постройте матрицу управления доступом для медицинского учреждения, в

котором врачи могут читать писать истории болезней и предписания по лечению, а медицинские сестры могут читать и писать предписания по лечению, но ничего не должны знать об истории болезней.

10. Оценивание результатов обучения и уровня сформированности компетенций

Оценивание результатов обучения по дисциплине операции и атаки в компьютерных системах сетях 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. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем[Электронный ресурс]: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - Москва: ИНФРА-М, 2021. -118 с. + Доп. материалы. - (Высшее образование: Бакалавриат).- Режим доступа: https://znanium.com/read?id=362430.

2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]: учебное пособие / В.Ф. Шаньгин. - Москва: ФОРУМ: ИНФРА- М, 2022. - 592 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Режим доступа: https://znanium.com/read?id=389857..

Дополнительная литература:

1. М. Ховард, Д. Лебланк Защищенный код. М.: ИД Русская редакция, 2004.− 704 с.

2. Проскурин В. Г. Защита программ и данных. М.: ИДАкадемия, 2012.− 208 с.

3. T. Howlett Open source security tools. Practical applications for security. Prantice Hall,2004.− 600 p.

4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие.− М.: ИД Форум – Инфра, 2013.− 416 с.

5. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. М.: Горячая линия – Телеком, 2000.− 452 с.

6. Хорев П. Б. Методы и средства защиты информации в компьютерных системах. М.: Академия, 2008.− 256 с.

7. Девянин П. Н. Модели безопасности компьютерных систем. Учебное пособие.−М.: Академия, 2005.− 144 с

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, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещениями для самостоятельной работы студентов.

Учебная аудитория для проведения занятий лекционного типа

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 практических занятий, 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.

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 №____