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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ АТАКАМ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Форма промежуточной аттестации: экзамен

2025

Рабочая программа по дисциплине «Системы противодействия компьютерным атакам» 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

Формирование и закрепление общепрофессиональных и профессиональных компетенций, направленных на знание и владение современными методами и технологиями противодействия информационным атакам и операциям, реализуемым в компьютерных системах и сетях.

Задачи:

- ознакомление с основными принципами построения систем противодействия компьютерным атакам, способами обнаружения и нейтрализации последствий вторжений в компьютерные системы;
- формирование умений анализировать защищенность компьютерных систем, управлять системами противодействия компьютерным атакам;
- приобретение навыков выявления и устранения уязвимостей компьютерных систем, настройки систем противодействия компьютерным атакам.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Системы противодействия компьютерным атакам» 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-3.5	Администрирование в Linux Математические методы защиты информации	**Системы противодействия компьютерным атакам**	

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-3.5. Способен разрабатывать требования по защите, формированию политик безопасности компьютерных систем и сетей на основе менеджмента, аудита и оценки рисков информационной безопасности	ПК-3.5.1. Принимает решения о необходимости защиты информации, содержащейся в ИС	Знать: основные принципы построения и механизмы функционирования систем противодействия компьютерным атакам, особы обнаружения и нейтрализации последствий вторжений в компьютерные системы. Уметь: анализировать защищенность компьютерных систем, управлять системами противодействия компьютерным атакам Владеть: навыками выявления и устранения уязвимостей компьютерных систем, настройки систем противодействия компьютерным атакам.
	ПК-3.5.2. Принимает решения о необходимости защиты информации, содержащейся в ИС	Знать: основные принципы построения и механизмы функционирования систем противодействия компьютерным атакам, особы обнаружения и нейтрализации последствий вторжений в компьютерные системы. Уметь: анализировать защищенность компьютерных систем, управлять системами противодействия компьютерным атакам Владеть: навыками выявления и устранения уязвимостей компьютерных систем, настройки систем противодействия компьютерным атакам.
	ПК-3.5.3. Анализирует компьютерную систему с целью определения необходимого уровня защищенности и доверия на основе менеджмента, аудита и оценки рисков информационной безопасности.	Знать: основные принципы построения и механизмы функционирования систем противодействия компьютерным атакам, особы обнаружения и нейтрализации последствий вторжений в компьютерные системы. Уметь: анализировать защищенность компьютерных систем, управлять системами противодействия компьютерным атакам Владеть: навыками выявления и устранения уязвимостей компьютерных систем, настройки систем

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
		противодействия компьютерным атакам.

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
			А
1. Контактная работа обучающихся с преподавателем:		69	69
Аудиторные занятия, часов всего, в том числе:		68	68
• занятия лекционного типа		34	34
• занятия семинарского типа:		34	34
практические занятия		34	34
лабораторные занятия		-	-
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		39	39
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		15	15
- выполнение индивидуальных заданий по практическим занятиям		15	15
- подготовка к экзамену		9	9
Промежуточная аттестация: экзамен		-	-
3. Контроль:		36	36
ИТОГО:	часов	144	144
общая трудоемкость	зач. ед.	4	4

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

5.1. Содержание дисциплины

Тема 1. Системный подход к обеспечению защиты от компьютерных атак

Компьютерные системы и их компоненты как объекты защиты от угроз безопасности.

Направления, методы и методики построения защищенных компьютерных систем.

Организационные методы и средства защиты компьютерных систем от атак

Тема 2. Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности

Методы и средства оценки защищенности, контроля доступа к компонентам компьютерных систем. Методы и средства обеспечения безопасности электропитания компьютерных систем, гарантированного уничтожения информации, выявления и локализации утечек информации по техническим каналам

Тема 3. Методы и средства обнаружения и отражения сетевых атак

Методы и средства обнаружения сетевых атак и вредоносных программ. Контентная фильтрация и межсетевое экранирование. Средства создания виртуальных частных сетей.

Тема 4. Комплексные средства защиты от компьютерных атак

Доверенные аппаратные среды. Подсистемы безопасности операционных систем, СУБД, прикладного программного обеспечения. Комплексные системы защиты локальных и корпоративных сетей. Системы контроля работы пользователей компьютерных систем. Оснащение центров Государственной системы обнаружения и противодействия компьютерным атакам РФ.

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. Системный подход к обеспечению защиты от компьютерных атак.	8	8/8	10	ПК-3.5, ПК-3.5.1, ПК-3.5.2, ПК3.5.3
2	Тема 2. Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности.	8	8/8	10	ПК-3.5, ПК-3.5.1, ПК-3.5.2, ПК3.5.3

№ 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	
3	Тема 3. Методы и средства обнаружения и отражения сетевых атак.	8	8/8	10	ПК-3.5, ПК-3.5.1, ПК-3.5.2, ПК3.5.3
4	Тема 4. Комплексные системы защиты от компьютерных атак	10	10/10	9	ПК-3.5, ПК-3.5.1, ПК-3.5.2, ПК3.5.3
	Всего	**34**	**34/34**	**39**	

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.	Тема 1. Системный подход к обеспечению защиты от компьютерных атак.	Системный подход к обеспечению защиты от компьютерных атак	8
2.	Тема 2. Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности.	Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности	8
3.	Тема 3. Методы и средства обнаружения и отражения сетевых атак.	Методы и средства обнаружения и отражения сетевых атак	8
4.	Тема 4. Комплексные системы защиты от компьютерных	Комплексные средства защиты от компьютерных атак	10

№ п/п	Наименование раздела, темы дисциплины	Содержание практических занятий	Объем (час.)
			Очная форма обучения
	атак		
	Всего		**34**

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Системы противодействия компьютерным атакам» 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 экзамену

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 промежуточно аттестации (экзамен)

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.
41. Классификация угроз безопасности компьютерным системам.
42. Системные принципы защиты информации в компьютерных системах.
43. Стратегические направления государственной политики России в сфере противодействия компьютерным атакам
44. Методика построения комплексной защиты компьютерных систем.
45. Информационные технологии, повышающие защищенность компьютерных систем.
46. Структура и функции ГосСОПКА.
47. Методика расследования компьютерных атак
48. Характеристика средств защиты целостности и бесперебойности функционирования компьютерных систем.
49. Методика организации защищенного электропитания компьютерных систем.
50. Методы и средства контроля эффективности защиты информации в компьютерных системах.

Образцы билетов

Билет №1

1. Правила NRU и NWD . Области использования этих правил.
2. Методы и средства контроля эффективности защиты информации в компьютерных системах
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 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. Лукацкий А.В. Обнаружение атак. - СПб.: BHV, 2003. -596 с.
2. Синадский Н. И., Хорьков Д. А. Защита информации в компьютерных сетях: учебное пособие . — Екатеринбург : УрГУ, 2008. -225с.
3. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). - М.: Горячая линия — Телеком, 2013, -220 с.
4. Новак Д., Норткатт С., Маклахен Д. Как обнаружить вторжение в сеть. 2016. -384 с.
5. Ларина Е.С., Овчинский В.С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. – М.: Книжный мир, 2014. -352 с.
6. Белоножкин В.И., Системы обнаружения компьютерных атак: учебное пособие. ВГТУ, 2015. [Эл.ресурс].
7. Мельников Д.А. Информационная безопасность открытых систем : учебник / Д.А. Мельников. — М.: ФЛИНТА : Наука, 2013. -448 с. Бабин С. А. Лаборатория хакера. — СПб.: БХВ-Петербург, 2016. -240 с.
8. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.
9. Остапенко А.Г. Сетео-информационная эпидемиология: учебное пособие для вузов. - М.: Горячая линия – Телеком, 2021. -216с. Дополнительная литература
10. М. Ховард, Д. Лебланк Защищенный код. М.: ИД Русская редакция, 2004.− 704 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 семинар, 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

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 №____