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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 9 з.е.
в академических часах: 324 ак.ч.

Форма промежуточной аттестации: экзамен

2025

Рабочая программа по дисциплине «Защита информации от утечки по техническим каналам» 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 естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

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 «Защита информации от утечки по техническим каналам» является формирование у обучающихся фундаментальных и прикладных знаний в области основ технической защиты информации от утечки по техническим каналам, а также формирование умений, навыков и компетенций по применению способов и средств технической защиты информации от утечки по техническим каналам, установление взаимосвязи и логической организации входящих в нее компонентов.

Задачи: целью преподавания и изучения дисциплины «Защита информации от утечки по техническим каналам» является формирование у обучающихся фундаментальных и прикладных знаний в области основ технической защиты информации от утечки по техническим каналам, а также формирование умений, навыков и компетенций по применению способов и средств технической защиты информации от утечки по техническим каналам, установление взаимосвязи и логической организации входящих в нее компонентов.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации от утечки по техническим каналам» 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
ОПК-5	Учебная практика,учебно-лабораторный практикум	Стандарты в сфере информационной безопасности	Производственная практика, преддипломная практика
ОПК-9	Автоматизация тестирования ПО	Защищенные информационные системы	Производственная практика, преддипломная практика -

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
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1. Применяет в профессиональной деятельности знания нормативной правовой базы РФ в области информационной безопасности	Знать: нормативные правовые акты Российской Федерации в области информационной безопасности Уметь: анализировать и применять эти документы в рамках профессиональной деятельности, обеспечивая соответствие требованиям законодательства и стандартов в области защиты информации. Владеть: навыками практического использования нормативной базы для разработки и реализации мер по защите информации.
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ОПК-9.1 Демонстрирует умение решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития компьютерных сетей	Знать: современные методы и средства защиты информации в операционных системах, компьютерных сетях, системах управления базами данных, а также способы предотвращения утечек информации по техническим каналам. Уметь: решать профессиональные задачи с учетом текущего состояния технологий и тенденций их развития, разрабатывать решения по защите информации в сетях и системах передачи данных. Владеть: навыками анализа угроз информационной безопасности и выбора оптимальных методов защиты с учетом специфики задач.

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	А
1. Контактная работа обучающихся с преподавателем:		138	69	69
Аудиторные занятия, часов всего, в том числе:		136	68	68
• занятия лекционного типа		68	34	34
• занятия семинарского типа:		68	34	34
практические занятия		-	-	-
лабораторные занятия		68	34	34
в том числе занятия в форме практической подготовки		-	-	-
Консультации		1	0,5	0,5
Контактные часы на аттестацию в период экзаменационных сессий		1	0,5	0,5
2. Самостоятельная работа студентов всего, в том числе		114	39	75
- подготовка курсовой работы		-	-	-
- проработка учебного (теоретического) материала		45	15	30
- выполнение домашних заданий по практическим занятиям		45	15	30
- подготовка к экзамену		24	9	15
Промежуточная аттестация: экзамен		72	36	36
ИТОГО:	часов	324		
общая трудоемкость	Зач.ед.	9		

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

5.1. Содержание дисциплины

Тема 1. Технические каналы утечки речевой информации

Классификация источников информации. Виды носителей информации. Основные и вспомогательные технические средства и системы. Источники опасных информативных сигналов. Демаскирующие признаки информационных объектов.

Тема 2. Технические каналы утечки информации, обрабатываемой СВТ

Создаваемые технические каналы утечки информации, обрабатываемой СВТ

Тема 3. Средства защиты информации от утечек по техническим каналам утечки речевой информации

Средства для проведения специальных проверок и исследований. Классификация средств обнаружения, локализации электрических каналов утечки речевой информации.

Тема 4. Средства защиты информации от утечек информации, обрабатываемой СВТ

Средства для проведения специальных проверок и исследований.

Классификация средств обнаружения, локализации электрических каналов утечки информации.

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)	самос-тоятельная работа	
1	Тема 1. Технические каналы утечки речевой информации	16	16/16	26	ОПК-5, ОПК-5.1, ОПК-9, ОПК-9.1
2	Тема 2. Технические каналы утечки информации, обрабатываемой СВТ	16	16/16	26	ОПК-5, ОПК-5.1, ОПК-9, ОПК-9.1
3	Тема 3. Средства защиты информации от утечек по техническим каналам утечки речевой информации	16	16/16	26	ОПК-5, ОПК-5.1, ОПК-9, ОПК-9.1
4	Тема 4. Средства защиты информации от утечек информации, обрабатываемой СВТ	20	20/20	36	ОПК-5, ОПК-5.1, ОПК-9, ОПК-9.1
	Всего	**68**	**68/68**	**114**	

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. Исследование акустоэлектрического канала утечки информации в среде Multisim с использованием закладного устройства в сети электропитания	Исследование акустоэлектрического канала утечки информации с использованием закладного устройства «Телефонное ухо». Компьютерные презентации и обсуждение Разбор конкретных ситуаций (задач) с использованием штатного ПО, выполнение тестов на знание терминологии, сведений из области информационной безопасности, программирование алгоритмов	16

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
2.	Тема 2. Исследование акустоэлектрических параметров ПЭМИ средств СВТ в среде Multisim	Исследование принципа работы нелинейного локатора в среде Multisim. Компьютерные презентации и обсуждение Разбор конкретных ситуаций (задач) с использованием штатного ПО, выполнение тестов на знание терминологии, сведений из области информационной безопасности, программирование алгоритмов	16
3.	Тема 3. Исследование электрических параметров СЗИ «Гранит-8» в среде Multisim	Компьютерные презентации и обсуждение Разбор конкретных ситуаций (задач) с использованием штатного ПО, выполнение тестов на знание терминологии, сведений из области информационной безопасности, программирование алгоритмов	16
4.	Тема 4. Исследование электрических параметров помехоподавляющих фильтров в среде Multisim	Исследование электрических параметров генераторов шума в среде Multisim. Компьютерные презентации и обсуждение Разбор конкретных ситуаций (задач) с использованием штатного ПО, выполнение тестов на знание терминологии, сведений из области информационной безопасности, программирование алгоритмов	20
	Всего		**68**

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Защита информации от утечки по техническим каналам» 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.

Текущий контроль включает контрольную работу по итогам первой половины курса.

Перечень вопросов к экзамену

1**. Технические каналы утечки информации**

1. Понятия информации, сообщения, носителя информации, защищаемой информации.
2. Основные угрозы безопасности и направления защиты информации; типовые последствия реализации угроз.
3. Понятие, структурная схема и основные характеристики технического канала утечки информации.
4. Распространённые классификации технических каналов утечки информации.
5. Основные угрозы безопасности информации по оптическому каналу утечки, способы их выявления и блокирования.
6. Основные угрозы безопасности информации по акустическому каналу утечки.
7. Применение систем лазерного зондирования как угроза безопасности защищаемой информации; способы выявления и нейтрализации.
8. Применение систем скрытого акустического контроля с подключением к абонентским телефонным линиям как угроза безопасности защищаемой информации; способы выявления и нейтрализации.
9. Применение систем скрытого акустического контроля с передачей данных по сети электропитания как угроза безопасности защищаемой информации; способы выявления и нейтрализации.
10. Методика технической защиты речевой информации; особенности распространения акустических волн, блокирования прямых и побочных акустических каналов.
11. Основные способы и средства выявления и блокирования акустических каналов утечки информации.
12. Основные способы и средства выявления и блокирования виброакустических каналов утечки информации.

13. Основные угрозы безопасности информации по электрическому каналу утечки.

14. Применение «проводных» микрофонов как угроза безопасности защищаемой информации; способы выявления и нейтрализации.

15. Акустоэлектрический эффект как угроза безопасности защищаемой информации; способы нейтрализации.

16. Электромагнитные наводки как угроза безопасности защищаемой информации; способы нейтрализации.

17. Паразитные электрические связи как угроза безопасности защищаемой информации; способы нейтрализации.

18. Опасные сигналы в цепях электропитания как угроза безопасности защищаемой информации; способы нейтрализации.

19. Опасные сигналы в цепях заземления как угроза безопасности защищаемой информации; способы нейтрализации.

20. Основные способы и средства выявления и блокирования электрических каналов утечки информации.

21. Основные угрозы безопасности информации по электромагнитному каналу утечки.

22. Применение систем скрытого акустического контроля с передачей данных по радиоканалу как угроза безопасности защищаемой информации; способы выявления и нейтрализации.

23. Высокочастотное навязывание как один из видов технической разведки; способы выявления и нейтрализации.

24. Физические основы экранирования электрических, магнитных и электромагнитных полей.

25. Основные способы и средства выявления и блокирования электромагнитных каналов утечки информации.

26. Особенности электромагнитного экранирования служебных помещений.

27. Основные технологии перехвата сообщений в проводных, радио и волоконнооптических линиях связи.

2. Средства защиты информации от утечек

28. Способы защиты информации от утечки в сетях связи: преобразование (скремблирование) аналоговых сигналов и цифровое шифрование.

29. Классификация и сущность основных способов преобразования (скремблирования) аналоговых сигналов в сетях связи; сравнительная характеристика.

30. Основные способы скремблирования: виды и характеристика частотных преобразований аналоговых сигналов в линиях связи.

31. Основные способы скремблирования: виды и характеристика временных преобразований аналоговых сигналов в линиях связи.

32. Распространённые способы энергетического скрытия аналоговых

сигналов телефонных систем связи.

33. Задачи и содержание основных этапов специальных проверок объектов информатизации.

34. Основные методы поисковой операции специальной проверки объекта информатизации.

35. Технические средства и способы контроля радиоэфира объекта информатизации.

36. Локаторы нелинейности; виды, принцип действия, особенности применения в сфере защиты информации.

37. Рефлектометры и анализаторы спектра; решаемые задачи, принцип действия, особенности применения в сфере защиты информации.

38. Защита информации в нормах законодательства Российской Федерации (цели защиты, виды защищаемой информации, субъекты защиты).

39. Информация, подлежащая защите в Российской Федерации; её источники и носители.

40. Теория разборчивости формант; инструментально-расчётный метод выявления акустических каналов утечки информации и оценки защищённости объекта информатизации.

Образцы билетов

1. Технические каналы утечки информации

Билет №1

1. Понятия информации, сообщения, носителя информации, защищаемой информации.

2. Основные угрозы безопасности информации по электромагнитному каналу утечки.

Билет №2

1. Основные угрозы безопасности и направления защиты информации; типовые последствия реализации угроз.

2. Применение систем скрытого акустического контроля с передачей данных по радиоканалу как угроза безопасности защищаемой информации; способы выявления и нейтрализации.

2. Средства защиты информации от утечек

Билет №1

1. Способы защиты информации от утечки в сетях связи: преобразование (скремблирование) аналоговых сигналов и цифровое шифрование.

2. Локаторы нелинейности; виды, принцип действия, особенности применения в сфере защиты информации.

Билет №2

1. Классификация и сущность основных способов преобразования (скремблирования) аналоговых сигналов в сетях связи; сравнительная характеристика.

2. Защита информации в нормах законодательства Российской Федерации (цели защиты, виды защищаемой информации, субъекты защиты).

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

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

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

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

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

6. 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

1. Лицензионное программное обеспечение, в том числе отечественного производства:

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

1. 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)

1. Профессиональные базы данных не используются.
2. 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, Лаборатория технической защиты информации

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

Технические средства обучения: персональный компьютер - 15, сетевое оборудование; специализированное оборудование по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок; технические средства контроля эффективности защиты информации от утечки по указанным каналам.

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 №____