Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Амурский государственный университет"

УТВЕРЖДАЮ
Проректор по учебной и научной работе
Лейфа А.В. Лейфа
19 июня 2024 г.

РАБОЧАЯ ПРОГРАММА
«ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки 09.03.01 Информатика и вычислительная техника

Направленность (профиль) образовательной программы – Информатика и вычислительная техника

Квалификация выпускника – Бакалавр

Год набора – 2024

Форма обучения – Очная

Курс 3,4 Семестр 6,7

Экзамен 7 сем

Зачет с оценкой 6 сем

Общая трудоемкость дисциплины 288.0 (академ. час), 8.00 (з.е)

Составитель С.Г. Самохвалова, доцент, канд. техн. наук

Институт компьютерных и инженерных наук

Кафедра информационной безопасности

2024

Рабочая программа составлена на основании Федерального государственного образовательного стандарта ВО для направления подготовки 09.03.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.17 № 929

Рабочая программа обсуждена на заседании кафедры информационной безопасности

01.02.2024 г. , протокол № 8

Заведующий кафедрой Никифорова Л.В. Никифорова

СОГЛАСОВАНО
Учебно-методическое управление
Чалкина Н.А. Чалкина
19 июня 2024 г.

СОГЛАСОВАНО
Выпускающая кафедра
Бушманов А.В. Бушманов
19 июня 2024 г.

СОГЛАСОВАНО
Научная библиотека
Петрович О.В. Петрович
19 июня 2024 г.

СОГЛАСОВАНО
Центр цифровой трансформации и технического обеспечения
Тодосейчук А.А. Тодосейчук
19 июня 2024 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины:

формирование у студентов знаний по основам инженерно- технической защиты информации, а также навыков и умения в применении знаний для конкретных условий.

Задачи дисциплины:

- изучение систем и средств инженерно- технической разведки, методов и способов организации защиты объектов активными и пассивными способами и техническими средствами, выбора оптимальных технических средств защиты информации, нормативно- методических и правовых документов, регламентирующих вопросы технической защиты информации;
- формирование умения выявлять каналы утечки на конкретных объектах и оценивать их возможности;
- формирование умения определять рациональные меры защиты на объектах и оценивать уровень эффективности их защиты.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к части, формируемая участниками образовательных отношений
образовательной программы. Данный курс базируется на знаниях, полученных в области сети и телекоммуникации, информационная безопасность, операционных систем, баз данных.
Знания, умения и навыки, полученные в процессе изучения данного курса, могут быть использованы студентами для подготовки выпускной квалификационной работы.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

3.1 Профессиональные компетенции и индикаторы их достижения

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
ПК 11 Способен обеспечивать информационную безопасность уровня баз данных	ИД-1ПК-11 Знать угрозы безопасности БД и способы их предотвращения, инструменты обеспечения безопасности БД и их возможности; ИД-2ПК-11 Уметь: выявлять угрозы безопасности на уровне БД, разрабатывать мероприятия по обеспечению безопасности на уровне БД; ИД-3ПК-11 Владеть навыками анализа возможных угроз для безопасности данных, навыками выбора средств поддержки информационной безопасности на уровне БД.
ПК 12 Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения. Способен проводить регламентные работы на сетевых устройствах и программном обеспечении	ИД-1ПК-12 Знать: архитектуру, устройство и функционирование вычислительных систем, коммуникационное оборудование, сетевые протоколы, методы обеспечения информационной безопасности; ИД-2ПК-12 Уметь: подготавливать протоколы мероприятий; ИД-3ПК-11 Владеть: практическими навыками администрирования инфокоммуникационной системы, проведение регламентных работ на сетевых

инфокоммуникационной системы	устройствах и программном обеспечении

4. СТРУКТУРА ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 8.00 зачетных единицы, 288.0 академических часов.

1 – № п/п

2 – Тема (раздел) дисциплины, курсовая работа (проект), промежуточная аттестация

3 – Семестр

4 – Виды контактной работы и трудоемкость (в академических часах)

4.1 – Л (Лекции)

4.2 – Лекции в виде практической подготовки

4.3 – ПЗ (Практические занятия)

4.4 – Практические занятия в виде практической подготовки

4.5 – ЛР (Лабораторные работы)

4.6 – Лабораторные работы в виде практической подготовки

4.7 – ИКР (Иная контактная работа)

4.8 – КТО (Контроль теоретического обучения)

4.9 – КЭ (Контроль на экзамене)

5 – Контроль (в академических часах)

6 – Самостоятельная работа (в академических часах)

7 – Формы текущего контроля успеваемости

1	2	3	4									5	6	7
			4.1	4.2	4.3	4.4	4.5	4.6	4.7	4.8	4.9			
1	Концепция инженерно-технической защиты информации	6	4				4						8	опрос
2	Теоретические основы инженерно-технической защиты информации	6	12				12						18	опрос
3	Технические средства добывания и инженерно-технической защиты информации	6	12				12						24	опрос
4	Средства предотвращения утечки информации по техническим каналам.	6	6				6						25.8	опрос

5	Организационные основы инженерно-технической защиты информации	7	12				12						44	опрос
6	Методическое обеспечение инженерно-технической защиты информации	7	6				4						30	опрос
7	Зачет с оценкой	6								0.2				
8	Экзамен	7									0.3	35.7		
	Итого		52.0		0.0		50.0		0.0	0.2	0.3	35.7	149.8	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Лекции

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
1	Концепция инженерно-технической защиты информации	Характеристика инженерно- технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно- технической защиты информации. Показатели эффективности инженерно-технической защиты информации.
2	Теоретические основы инженерно- технической защиты информации	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Образование опасных сигналов в результате побочных электромагнитных излучений и наводок. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально- вещественные каналы утечки информации, их характеристика и возможности. Методы инженерной защиты и технической охраны объектов. Классификация способов инженерной защиты и технической охраны объектов. Инженерные конструкции. Автономные и централизованные системы охраны. Подсистемы обнаружения злоумышленника и пожара, видеоконтроля, нейтрализации угроз и

		управления охраной.
3	Технические средства добывания и инженерно-технической защиты информации	Визуально- оптические приборы. Фотоаппараты. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом. Классификация и характеристика охранных, охранно- пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.
4	Средства предотвращения утечки информации по техническим каналам.	Средства маскировки и дезинформации в оптическом и радиодиапазонах. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления.
5	Организационные основы инженерно- технической защиты информации	Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств. Виды контроля эффективности инженерно- технической защиты информации. Виды зон безопасности. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации.
6	Методическое обеспечение инженерно- технической защиты информации	Основные этапы проектирования и оптимизации системы инженерно- технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно- технической защиты информации. Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в помещении. Принципы оценки размеров зон I и II. Оценка дальности перехвата сигналов.

5.2. Лабораторные занятия

Наименование темы	Содержание темы
Концепция инженерно-технической защиты информации	Системный подход к защите информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения.
Теоретические основы инженерно- технической защиты информации	Средства инженерно-технической защиты и технической охраны Распространение сигналов в технических каналах утечки информации
Технические средства добывания и инженерно-технической защиты информации	Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания
Средства предотвращения утечки информации по техническим каналам.	Средства предотвращения утечки информации по техническим каналам Физические основы утечки информации по каналу побочных электромагнитных излучений и наводок
Организационные основы инженерно- технической защиты информации	Определение основных показателей эффективности инженерно-технической защиты информации Контроль эффективности инженерно- технической защиты информации
Методическое обеспечение инженерно- технической защиты информации	Моделирование процессов инженерно- технической защиты информации

6. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)	Трудоемкость в академических часах
1	Концепция инженерно-технической защиты информации	Подготовка к лекциям и лабораторным занятиям.	8
2	Теоретические основы инженерно-технической защиты информации	Подготовка к лекциям и лабораторным занятиям.	18
3	Технические средства добывания и инженерно-технической защиты информации	Подготовка к лекциям и лабораторным занятиям.	24
4	Средства предотвращения утечки информации по техническим каналам.	Подготовка к лекциям и лабораторным занятиям.	25.8

5	Организационные основы инженерно-технической защиты информации	Подготовка к лекциям и лабораторным занятиям.	44
6	Методическое обеспечение инженерно-технической защиты информации	Подготовка к лекциям и лабораторным занятиям.	30

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе подготовки по дисциплине используется совокупность методов и средств обучения, позволяющих осуществлять целенаправленное методическое руководство учебно-познавательной деятельностью бакалавров, в том числе на основе интеграции информационных и традиционных педагогических технологий.

На занятиях используются методы активного обучения: лекция с заранее запланированными ошибками (лекция- провокация), лекция с разбором конкретных ситуаций, мозговой штурм. Рекомендуется использование информационных технологий при организации коммуникации со студентами для представления информации, выдачи рекомендаций и консультирования по оперативным вопросам (электронная почта), использование мультимедиа- средств при проведении лекционных, практических и лабораторных занятий.

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6 семестр

Промежуточная аттестация по итогам освоения дисциплины: зачет с оценкой

Вопросы к зачету

1. Понятие информации. Виды представления и классификация информации.
2. Понятия безопасности и системы безопасности информации. Системный подход к защите информации.
3. Угрозы конфиденциальной информации и их классификация.
4. Источники угроз безопасности информации, их классификация и ранжирование.
5. Инженерно-техническая защита информации.
6. Классификация и общая характеристика каналов утечки информации.
7. Технические каналы утечки информации и их образование.
8. Классификация и характеристика каналов утечки речевой информации.
9. Технические каналы утечки речевой информации и методы ее съема.
10. Технические средства съема аудиоинформации. Микрофоны и их виды.
11. Методы съема информации в телефонных линиях связи.
12. Технические средства съема видеоинформации и их общая характеристика.
13. Методы и средства съема информации по радиоканалу.
14. Методы и средства съема информации телевизионной и вычислительной техники.
15. Методы и средства съема информации в высокочастотных и волоконно-оптических кабелях.
16. Защита речевой информации с помощью маскирующих сигналов.
17. Системы виброакустического зашумления.
18. Защита речевой информации от лазерного съема.
19. Методы и средства обнаружения радиозакладных устройств. Индикаторы поля, панорамные сканирующие приемники, аппаратно-программные ком-плексы.
20. Методы и средства обнаружения радиозакладных устройств. Обнаружители диктофонов и нелинейные радиолокаторы.
21. Общие принципы защиты телефонных линий связи. Методы и средства пассивной защиты.
22. Методы подавления телефонных закладных устройств.
23. Методы и средства обнаружения и противодействия в телефонных линиях связи.

24. Общая характеристика методов защиты информации от утечки по электромагнитным каналам.
25. Защита линий связи. Защита информации от утечки в волоконно- оптических линиях связи.
26. Защита информации от утечки за счет микрофонного эффекта.
27. Защита информации от утечки за счет электромагнитного излучения.
28. Защита информации от утечки за счет паразитной генерации, по цепям пи-тания и по цепям заземления.
29. Защита информации от утечки за счет взаимного влияния проводов и линий связи и высокочастотного навязывания.
30. Использование специализированных пленок, тканей, эмалей и ферритовых фильтров для защиты информации от утечки по электромагнитным каналам.
31. Детекторы видеокамер.
32. Применение радиоэлектронных помех для защиты информации от утечки по электромагнитному каналу.

7 семестр
Промежуточная аттестация по итогам освоения дисциплины: экзамен
Вопросы к экзамену

1. Методы дистанционного проникновения в помещение для скрытого съема аудио - и видеоинформации.
2. Экранирование технических средств и помещений.
3. Звукоизоляция помещений.
4. Экранирование технических средств и помещений.
5. Использование специализированных пленок, тканей, эмалей и ферритовых фильтров для защиты информации от утечки по электромагнитным кана-лам.
6. Детекторы видеокамер.
7. Применение радиоэлектронных помех для защиты информации от утечки по электромагнитному каналу.
8. Уязвимости безопасности информации, их классификация и ранжирование.
9. Действия, приводящие к неправомерному овладению конфиденциальной информацией.
10. Правовая и организационная защита информации.
11. Термины и определения, основные нормативные и правовые документы по инженерно-технической защите объектов
12. Понятие системного подхода, основные методы при моделировании системы защиты информации, сущность системного подхода.
13. Основные положения по построению системы инженерно- технической защиты информации: многозональность пространства, равнопрочность рубежа контролируемой зоны, надежность технических средств системы защиты информации.
14. Мероприятия организационной защиты.

9. УЧЕБНО- МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) литература

1. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно- библиотечная система.

— URL: https:// e.lanbook.com/ book/293009 (дата обращения: 28.03.2024). — Режим доступа: для авториз. пользователей.
2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/ bcode/537247 (дата обращения: 28.03.2024).
3. Иванов, А. В. Защита речевой информации от утечки по акустоэлектрическим каналам : учебное пособие / А. В. Иванов, В. А. Трушин. — Новосибирск : Новосибирский государственный технический университет, 2012. — 43 с. — ISBN 978-5-7782-1888-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https:// www.iprbookshop.ru/44919.html (дата обращения: 28.03.2024). — Режим доступа: для авторизир. пользователей
4.Сагдеев, К. М. Физические основы защиты информации : учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. — Ставрополь : Северо- Кавказский федеральный университет, 2015. — 394 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https:// www.iprbookshop.ru/63152.html (дата обращения: 28.03.2024). — Режим доступа: для авторизир. пользователей
5. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко. — Ставрополь : Северо-Кавказский федеральный университет, 2015. — 222 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/63138.html (дата обращения: 28.03.2024). — Режим доступа: для авторизир. пользователей

б) программное обеспечение и Интернет-ресурсы

№	Наименование	Описание
1	Google Chrome	Бесплатное распространение по лицензии google chromium http:// code.google.com/ intl/ ru/ chromium/ terms.html на условиях https:// www.google.com/ chrome/ browser/privacy/eula_text.html.
2	LibreOffice	Бесплатное распространение по лицензии GNU LGPL https://ru.libreoffice.org/about-us/license/
3	Операционная система Linux	GNU-лицензия (GNU General Public License)
4	Система защиты информации от несанкционированного доступа Dallas Lock	Договор о сотрудничестве с образовательным учреждением 127-17-153/1.
5	Программный комплекс «КонсультантПлюс»	Лицензия коммерческая по договору №21 от 29 января 2015 года.
6	https:// www.iprbookshop.ru/	Цифровой образовательный ресурс IPR SMART — библиотечная система и удобные инструменты для обучения и преподавания на одной платформе
7	http://amursu.ru	Образовательный портал АмГУ
8	https://urait.ru	Электронная библиотечная система «Юрайт». Фонд электронной библиотеки составляет более 4000 наименований и постоянно пополняется новинками, в большинстве своем это учебники и учебные пособия для всех уровней профессионального образования от

		ведущих научных школ с соблюдением требований новых ФГОС.

в) профессиональные базы данных и информационные справочные системы

№	Наименование	Описание
1	http:// www.habrahabr.ru/	Интернет-портал для ИТ-специалистов
2	http://www.sec.ru	Интернет- портал обзора рынка технических средств безопасности
3	http://www.intuit.ru	Интернет-портал образовательных ресурсов по ИТ
4	http//www.all-ib.ru	Интернет- портал ресурсов по информационной безопасности
5	http://www.fstec.ru/	Официальный сайт Федеральной службы по техническому и экспортному контролю

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Занятия по дисциплине проводятся в специальных помещениях, представляющих собой учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Все помещения, в которых проводятся занятия, соответствуют действующим противопожарным правилам и нормам.

Каждый обучающийся обеспечен индивидуальным неограниченным доступом к электронно- библиотечным системам и к электронной информационно-образовательной среде университета.

Самостоятельная работа обучающихся осуществляется в помещениях, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно- образовательную среду университета.