Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.38 Защита информации от утечки по техническим каналам»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
10.03.01 Информационная безопасность
(код и наименование направления подготовки)

Безопасность автоматизированных систем (информационные технологии и электронная промышленность)
(наименование направленности (профиля) образовательной программы)

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2025

Рабочая программа дисциплины «*Б1.Д.Б.38 Защита информации от утечки по техническим каналам*» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 8 от "27" 03 20 25 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации В.В. Тугов
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
доцент кафедры ВТиЗИ Н. П. Мошуров
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность В.В. Тугов
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
С.Н. Морозова
личная подпись *расшифровка подписи*

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:
формирование у студентов практических навыков организации и проведения мероприятий по выявлению возможных технических каналов утечки информации на объектах информатизации и в выделенных помещениях и построения системы технической защиты.

Задачи:
− изучение способов и средств защиты информации, обрабатываемой техническими средствами;
− изучение способов и средств защиты информации от наблюдения;
− изучение способов и средств защиты выделенной информации от перехвата;
− изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
− изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
− изучение методов и средств оценки защищенности выделенных (защищаемых) помещений и соответствия их нормативным документам;
− обучение основам построения системы технической защиты информации на объектах информатизации и в выделенных помещениях.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.6 Основы информационной безопасности, Б1.Д.Б.14 Физика, Б1.Д.Б.15.1 Алгебра и геометрия, Б1.Д.Б.15.2 Математический анализ, Б1.Д.Б.16 Основы экономики и финансовой грамотности, Б1.Д.Б.26 Аппаратные средства вычислительной техники*

Постреквизиты дисциплины: *Б1.Д.Б.33 Комплексные системы защиты информации на предприятии, Б1.Д.Б.34 Проектирование систем информационной безопасности*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1-В-1 Применяет философские основы познания и логического мышления, методы научного познания, в том числе методы системного анализа, для решения поставленных задач УК-1-В-2 Осуществляет критический анализ и синтез информации, полученной из разных источников УК-1-В-3 Понимает основные закономерности и главные особенности социально-исторического развития различных культур в этическом и	**Знать:** − основы критического анализа и синтеза информации; − основные характеристики информации и требования, предъявляемые к ней; − источники информации, требуемой для решения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	философском контексте УК-1-В-4 Применяет методы сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий для решения поставленных задач УК-1-В-5 Формулирует и аргументирует выводы и суждения, в том числе с применением философского понятийного аппарата УК-1-В-6 Формулирует собственную гражданскую и мировоззренческую позицию с опорой на системный анализ философских взглядов и исторических закономерностей, процессов, явлений и событий	поставленной задачи; − основные различия между фактами, мнениями, интерпретациями и оценками; − возможные варианты решения типичных задач. **Уметь:** − выделять базовые составляющие поставленных задач; − критически работать с информацией; − использовать различные типы поисковых запросов; − использовать различные типы поисковых запросов; − формировать собственное мнение о фактах, мнениях, интерпретациях и оценках информации; − обосновывать варианты решений поставленных задач. **Владеть:** − методами анализа и синтеза в решении задач; − способностью определять, интерпретировать и ранжировать информацию; − способностью поиска информации; − способностью формировать и аргументировать свои выводы и суждения; способностью предлагать варианты решения поставленной задачи и оценивать их достоинства и недостатки.
ОПК-4.1 Способен проводить организационные	ОПК-4.1-В-1 Организует и проводит аудит, модернизацию, разработку и	**Знать:** − нормативные

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
мероприятия по обеспечению безопасности информации в автоматизированных системах	внедрение систем защиты информации	правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации от утечки по техническим каналам; – методы и методики контроля защищенности информации от утечки по техническим каналам; – отчетные документы, оформляемые по результатам контроля защищенности информации от утечки по техническим каналам. **Уметь:** – проводить оценку защищенности информации от утечки по техническим каналам; – оформлять отчетные материалы по результатам контроля защищенности информации от утечки по техническим каналам; – оформлять аттестат соответствия выделенных помещений требованиям по защите информации от утечки по техническим каналам. **Владеть:** – навыком подготовки отчетных материалов по результатам контроля защищенности информации от утечки по техническим каналам; навыком разработки (модернизации) систем защиты информации.
ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию,	ОПК-4.3-В-1 Планирует порядок и осуществляет необходимые работы по установке, настройке , обслуживанию и проверке работоспособности отдельных	**Знать:** – принципы построения средств защиты информации от

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	"утечки" по техническим каналам; – основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации от утечки по техническим каналам; – программно-аппаратные средства защиты информации от утечки по техническим каналам; – руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации от утечки по техническим каналам. **Уметь:** – использовать технические методы и средства защиты информации от утечки по техническим каналам; – планировать политику безопасности информации в части, касающейся ее утечки по техническим каналам; – классифицировать и оценивать угрозы утечки информации по техническим каналам; – применять программные средства защиты информации от утечки по техническим каналам; – устранять известные уязвимости, приводящие к возникновению каналов утечки информации; применять нормативные документы по противодействию технической разведке. **Владеть:**

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		– навыками обеспечения защиты информации от утечки по техническим каналам с учетом требования эффективного функционирования объекта информатизации; – навыками обнаружения неисправностей в работе системы защиты информации от утечки по техническим каналам; – навыками устранения неисправностей в работе системы защиты информации от утечки по техническим каналам; навыками наладки технических средств системы защиты информации от утечки по техническим каналам.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа).

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**71**	**71**
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)	34	34
Консультации	1	1
Индивидуальная работа и инновационные формы учебных занятий	1,5	1,5
Промежуточная аттестация (зачет, экзамен)	0,5	0,5
Самостоятельная работа: *- выполнение курсового проекта (КП);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- изучение разделов курса «Защита информации от утечки по техническим каналам» в системе электронного обучения;* *- подготовка к лабораторным занятиям;*	**73** +	**73**

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
- подготовка к практическим занятиям; *- подготовка к рубежному контролю)*		
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Способы и средства защиты информации от наблюдения	22	4	2	2	14
2	Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	28	4	2	4	18
3	Методы и средства выявления электронных устройств негласного получения информации	40	4	2	16	18
4	Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам	34	4	2	12	16
5	Организационные и технические меры инженерно-технической защиты информации	20	2	8		10
	Итого:	144	18	16	34	76
	Всего:	144	18	16	34	76

4.2 Содержание разделов дисциплины

Раздел №1 Способы и средства защиты информации от наблюдения

Способы и принципы работы средств защиты информации от наблюдения. Способы и средства противодействия наблюдению в оптическом диапазоне волн. Способы информационного скрытия объектов от радиолокационного наблюдения.

Раздел №2 Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Классификация объектов информатизации. Экранирование технических средств их соединительных линий. Экранированные помещения. Заземление технических средств. Требования к системам электропитания и заземления основных технических средств и систем. Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по установке). Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке).

Раздел №3 Методы и средства выявления электронных устройств негласного получения информации

Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства. Средства выявления электронных устройств негласного получения информации: индикаторы электромагнитного поля, программно-аппаратные комплексы радиоконтроля, анализаторы проводных коммуникаций, нелинейные локаторы, рентгено-телевизионные комплексы. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации. Способы и принципы работы средств защиты информации от перехвата. Методы и средства пассивного подавления опасных сигналов акустоэлектрических преобразователей.

Раздел №4 Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам

Способы и принципы работы средств защиты информации от подслушивания. Классификация, сущность и параметры звукоизоляции ограждений, кабин, акустических экранов, глушителей. Способы и средства предотвращения утечки информации с помощью закладных устройств. Показатели эффективности защиты речевой информации. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции. Методика расчета словесной разборчивости речи. Методика оценки возможностей средств акустической разведки по перехвату речевой информации. Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.

Раздел №5 Организационные и технические меры инженерно-технической защиты информации. Контроль эффективности защиты информации.

Организационные и технические меры инженерно-технической защиты информации. Контроль эффективности защиты информации. рекомендации по выбору средств защиты.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1.	3	Имитатор сигналов «Шиповник-2».	2
2.	3	Скоростной поисковый приемник радиосигналов «Скорпион»	2
3.	3	Многофункциональный поисковый прибор ST-031 «Пиранья»	4
4.	3	Поиск каналов утечки информации с помощью детектора поля DP- 20	2
5.	3	Поиск каналов утечки информации с помощью индикатора поля ST 110. Поиск и обнаружение радиозакладок в помещении	2
6.	2	Система виброакустической защиты (СВАЗ) Соната.	2
7.	2	Установка и настройка ПАК «Соболь»	2
8.	3	Работа с оптическим обнаружителем скрытых видеокамер Оптик. Работа с автоматическим обнаружителем видеокамер Айрис IQ-2V.	4
9.	1	Система охранно-тревожной сигнализации. Система контроля и управления доступом.	2
10.	4	Система оценки защищенности выделенных помещений по акустическому и виброакустическому каналу «Шепот»	6
11.	4	Автоматизированная система оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН) «Сигурд».	6
		Итого:	34

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1.	1	Способы и средства защиты информации от наблюдения	2
2.	2	Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	2
3.	3	Методы и средства выявления электронных устройств негласного получения информации	2
4.	4	Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по	2

№ занятия	№ раздела	Тема	Кол-во часов
		техническим каналам	
5.	5	Организация технической защиты информации	2
6.	5	Методические рекомендации по разработке мер защиты	2
7.	5	Организационные и технические меры инженерно-технической защиты информации в государственных и коммерческих структурах.	2
8.	5	Контроль эффективности защиты информации	2
		Итого:	16

4.5 Курсовой проект (6 семестр)

Проектирование системы технической защиты информации объекта информатизации.
Тема (предприятие, организация, учреждение) уточняется по согласованию с преподавателем.

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

5.1 Основная литература

1. Титов, А. А. Инженерно-техническая защита информации: учебное пособие / А. А. Титов. — Москва : ТУСУР, 2010. — 197 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4959

2. Голиков, А. М. Защита информации от утечки по техническим каналам: учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328

5.2 Дополнительная литература

1. Торокин, А. А. Инженерно-техническая защита информации [Текст] : учеб.пособие для вузов / А. А. Торокин. - М. : Гелиос АРВ, 2005. - 960 с.

2. Данилов, А. Н. Инженерно-техническая защита информации : учебное пособие / А. Н. Данилов, А. Л. Лобков. — Пермь : ПНИПУ, 2007. — 340 с. — ISBN 978-5-88151-821-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/160366

3. Титов, А. А. Технические средства защиты информации : учебное пособие / А. А. Титов. — Москва : ТУСУР, 2010. — 194 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4960

5.3 Периодические издания

Информация и безопасность: журнал. - Москва: Агентство "Роспечать",2009.
Информация и безопасность: журнал. - Москва: Агентство "Роспечать",2010.
Информация и безопасность: журнал. - Москва: Агентство "Роспечать",2013.
Вестник компьютерных и информационных технологий: журнал. - М.: Агентство "Роспечать", 2019.
Вестник компьютерных и информационных технологий: журнал. - М.: Агентство "Роспечать", 2018.

5.4 Интернет-ресурсы

http://www.analitika.info Средства защиты информации. Каталог техники выявления и противодействия средствам разведки, антитеррора. Форум по вопросам защиты информации.

http://www.fstec.ru Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России).

http://www.fsb.ru Федеральная Служба безопасности Российской Федерации.

http://clsz.fsb.ru Центр по лицензированию, сертификации и защите государственной тайны ФСБ России.

http://www.consultant.ru Общероссийская Сеть распространения правовой информации КонсультантПлюс

http://www.bnti.ru/about.asp Бюро научно-технической информации. Техника для спецслужб

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Операционная система РЕД ОС.
2. Пакет офисных приложений LibreOffice.
3. Университетская платформа электронного обучения «Электронные курсы ОГУ в системе обучения Moodle» (http://moodle.osu.ru).
4. Яндекс.Браузер - браузер, созданный компанией «Яндекс» (бесплатная версия) Режим доступа: https://browser.yandex.ru.
5. DION - платформа для проведения онлайн мероприятий и видеоконференций (конфигурация DION EDU).
6. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2025]. Режим доступа: http://garant.net.osu.ru.
7. КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2025].

6 Материально-техническое обеспечение дисциплины

Занятие лекционного типа проводятся в учебной аудитории, предназначенной для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Аудитория оборудована комплектами ученической мебели, доской, экраном DRAPER LUMA 120 - 1 шт., проектором модели EPSON EMP-S42 – 1 шт., Ко

Лабораторные занятия проводятся в компьютерных классах, предназначенных для проведения занятий лабораторного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. и лаборатория технической защиты информации и средств охранно-пожарной сигнализации

Ноутбук Dell Inspiron 5050-8189 Blach 15.6" Led (1366x768)/Core i3-2350M;

- Видеокамера цветная купольная NOVIcam 85A;
- Шиповник-2 (имитатор сигналов средств нелегального съема информации многофункциональный);
- Фильтр сетевой помехоподавляющий ФСПК 10,10А серт. ФСТЭК России 0617500;
- Устройство защиты цифровых ТА «МП-1Ц»; Скорпион вер.3,5 (скоростной приемник 30-20000МГц);
- Подавитель сотовых телефонов "Мозаика-Т";
- Оптик (оптический обнаружитель скрытых видеокамер, бинокуляр);
- ДСВЧИ 031 (детектор СВЧ излучений);
- ДП-20 (индикатор поля 2-31ГГц);
- Детектор поля ST 110;
- Test-031 (универсальный
- имитатор сигналов);

- ST-031P "Пиранья";
- Система оценки защищенности выделенных помещений по акустическому и виброакустическому каналу «Шепот»;
- Автоматизированная система оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН) «Сигурд».

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.