Минобрнауки России

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

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.20 Техническая защита информации»

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

2207909

Рабочая программа дисциплины «*Б1.Д.Б.20 Техническая защита информации*» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 8 от "21" 03 2025 г.

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

Исполнители:

доцент 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 института
С.Н. Морозова
личная подпись *расшифровка подписи*

№ регистрации _____

© Мошуров Н.П., 2025
© ОГУ, 2025

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

формирование у студентов знаний по основам организации и проведения мероприятий по выявлению возможных технических каналов утечки информации на объектах информатизации и в выделенных помещениях.

Задачи:

– ознакомление с видами и основными характеристиками защищаемой информации;
– ознакомление с основными источниками и носителями информации различных видов;
– изучение демаскирующих признаков объектов защиты;
– ознакомление с угрозами безопасности информации;
– изучение принципов добывания информации;
– ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
– обучение основам организации 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.15.2 Математический анализ, Б1.Д.Б.24 Языки программирования, Б1.Д.Б.27 Электротехника, Б1.Д.Б.28 Электроника и схемотехника*

Постреквизиты дисциплины: *Б1.Д.Б.30 Защита информационных процессов в автоматизированных системах, Б1.Д.Б.33 Комплексные системы защиты информации на предприятии, Б1.Д.Б.34 Проектирование систем информационной безопасности, Б1.Д.В.4 Лицензирование и сертификация в области защиты информации*

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-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8-В-1 Формирует культуру безопасного и ответственного поведения в повседневной жизни и профессиональной деятельности, обеспечивая безопасные и/или комфортные условия жизнедеятельности, труда на рабочем месте, в т.ч. с помощью средств защиты УК-8-В-2 Использует приемы первой помощи, методы защиты в условиях чрезвычайных ситуаций и военных конфликтов УК-8-В-3 Идентифицирует угрозы (опасности) природного и техногенного	**<u>Знать:</u>** – факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений); – правила поведения при возникновении

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	происхождения для жизнедеятельности человека и природной среды УК-8-В-4 В случае возникновения чрезвычайных ситуаций и военных конфликтов применяет методы защиты жизнедеятельности человека, принимает участие в спасательных и неотложных аварийно-восстановительных мероприятиях	чрезвычайных ситуаций природного и техногенного происхождения, оказания первой помощи и способы участия в восстановительных мероприятиях. **<u>Уметь:</u>** – анализировать факторы вредного влияния на жизнедеятельность элементов среды обитания; соблюдать и разъяснять правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения, оказывать первую помощь и участвовать в восстановительных мероприятиях
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10-В-1 Проводит экспертизу и разработку политики безопасности , организует и поддерживает выполнение комплекса мер по обеспечение информационной безопасности, управляет процессом их реализации в автоматизированных системах	**<u>Знать:</u>** – принципы построения средств 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. **<u>Уметь:</u>** – использовать техни-ческие методы и средства защиты информации от утечки по техническим каналам; – планировать политику

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		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. **<u>Владеть:</u>** – навыками обеспечения защиты информации от утечки по техническим каналам с учетом требования эффективного функционирования объекта защиты; – 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.
ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11-В-1 Планирует, проводит эксперименты и обрабатывает их результаты с использованием современных инструментальных средств ОПК-11-В-2 Умеет проводить эксперименты по заданной методике, осуществлять обработку и оценку погрешности и достоверности результатов экспериментов	**<u>Знать:</u>** – технические каналы утечки информации; – методы и методики контроля защищенности информации от утечки по техническим каналам; – порядок аттестации объектов информатизации на соответствие

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		требованиям по технической защите информации; – отчетные документы, оформляемые по результатам аттестации объектов информатизации на соответствие требованиям по технической защите информации; – способы защиты технических средств обработки информации. **<u>Уметь:</u>** – разрабатывать программы и методики аттестации испытаний выделенных помещений на соответствие требований по технической защите информации; – разрабатывать программы и методики сертификации технических средств защиты информации, проводить аттестационные испытания и оформлять документацию в соответствии с требованиями технической защиты информации; – оформлять аттестат соответствия выделенных помещений требованиям по технической защите информации, оформлять материалы аттестационных испытаний. **<u>Владеть:</u>** – навыками разработки программ и методик испытаний технических средств защиты информации;

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		– навыками проведения испытаний по методикам оценки защищенности объектов информатизации; навыками подготовки протокола испытаний и технического заключения по результатам испытаний.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	5 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**51,25**	**51,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)	16	16
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- изучение разделов курса «Техническая защита информации» в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю)*	**56,75**	**56,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 5 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Сущность и задачи технической защиты информации	8	2			6
2	Классификация и структура технических каналов утечки информации. Характеристики	66	10	16	22	18

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
	каналов утечки информации.					
3	Системный подход к инженерно-технической защите информации	8	2			6
4	Разработка системы технической защиты информации	26	4		12	10
	Итого:	108	18	16	34	40
	Всего:	108	18	16	34	40

4.2 Содержание разделов дисциплины

Раздел 1 Сущность и задачи технической защиты информации.

Цель и задачи технической защиты информации. Основные понятия и определения технической защиты информации. Законодательство РФ, регламентирующее техническую защиту информации. Государственные органы (регуляторы) координирующие работу по технической защите информации.

Раздел 2 Классификация и структура технических каналов утечки информации. Характеристики каналов утечки информации.

Демаскирующие признаки объектов. Виды и структура технических каналов утечки информации. Характеристики каналов утечки информации. Структура оптического канала утечки информации. Характеристики среды распространения оптических лучей. Основные показатели оптоэлектронных линий связи и способы снятия с них информации. Особенности радиоэлектронных каналов утечки информации. Виды и структура радиоэлектронных каналов утечки информации. Направляющие линии связи, их характеристики. Общая характеристика технических каналов утечки информации, обрабатываемой средствами вычислительной техники. Электромагнитные каналы утечки информации, обрабатываемой средствами вычислительной техники. Электрические каналы утечки информации. Специально создаваемые технические каналы утечки информации. Классификация акустических каналов утечки информации. «Заходовые» методы снятия информации. «Беззаходовые» методы снятия информации. Структура материально-вещественного канала утечки информации и характеристики ее элементов. Способы утечки демаскирующих веществ в твердом, жидком и газообразном виде. Особенности утечки информации о радиоактивных веществах.

Раздел 3 Системный подход к инженерно-технической защите информации

Системный подход к инженерно-технической защите информации. Сущность системного подхода и системного анализа. Основные этапы проектирования системы защиты информации техническими средствами. Принципы моделирования объектов защиты и технических каналов утечки информации.

Раздел 4 Разработка системы технической защиты информации

Разработка технической системы защиты информации объекта. Моделирование объектов защиты. Моделирование угроз и каналов утечки информации. Рекомендации по выбору методов и средств технической защиты информации. САПР систем технической защиты информации.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1.	2	Средства перехвата информации в оптическом диапазоне волн.	2
2.	2	Средства перехвата информации в радиоэлектронном и электромагнитном диапазонах волн.	4
3.	2	Средства перехвата информации в акустическом диапазоне волн.	2
4.	2	Средства перехвата информации в каналах, образованных средствами вычислительной техники.	4

5.	2	Средства добывания информации в материально-вещественном канале утечки	2
6.	4	Моделирование объекта защиты	4
7.	4	Моделирование технических каналов утечки информации	4
8.	4	Организация аттестации выделенного помещения по требованиям безопасности информации	4
9.	2	Комплексы пеленгации и радио мониторинга	4
10.	2	Аппаратура поиска технических средств разведки	4
		Итого:	34

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1.	2	Виды информации, защищаемой техническими средствами	2
2.	2	Демаскирующие признаки объектов защиты	2
3.	2	Источники и носители информации, защищаемой техническими средствами. Принципы записи и съема информации с носителей	2
4.	2	Источники опасных сигналов	2
5.	2	Виды угроз безопасности информации, защищаемой техническими средствами	2
6.	2	Органы добывания информации	2
7.	2	Способы несанкционированного доступа к источникам информации	2
8.	2	Основные способы и принципы работы средств добывания информации техническими средствами. Основные способы и средства наблюдения.	2
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

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

4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Текст] : учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей "Информатика и вычислительная техника" / В. Ф. Шаньгин. - Москва : Форум : ИНФРА-М, 2014. - 416 с. : ил. - Библиогр.: с. 401-408. - ISBN 978-5-8199-0331-5. - ISBN 978-5-16-003132-3.

5. Проскурин, В. Г. Защита программ и данных [Текст] : учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки 090900 "Информационная безопасность" (бакалавр) и специальностям 090301 "Компьютерная безопасность", 090303 "Информационная безопасность автоматизированных систем" / В. Г. Проскурин.- 2-е изд., стер. - Москва : Академия, 2012. - 208 с. : ил. - (Высшее профессиональное образование. Бакалавриат). - Библиогр.: с. 195-196. - ISBN 978-5-7695-9288-1.

5.3 Периодические издания

Журналы:
– InformationSecurity/Информационная безопасность;
– Проблемы информационной безопасности. Компьютерные системы;
– Защита информации. Инсайд;

5.4 Интернет-ресурсы

1. http://www.fsb.ru – сайт ФСБ РФ
2. http://www.fstec.ru – сервер ФСТЭК РФ
3. http://www.gov.ru – сервер органов государственной власти РФ
4. http://www.minsvyaz.ru – сайт министерства информационных технологий и связи РФ
5. http://www.scrf.gov.ru – сайт Совета Безопасности РФ
6. www.consultant.ru – Консультант плюс
7. https://gost.ru – Росстандарт
8. http://docs.cntd.ru – Электронный фонд правовой и нормативно-технической документации
9. http://www.securrity.ru – Сайт Информационная безопасность
10. https://www.securitylab.ru – Информационный портал по информационной безопасности
11. https://securelist.ru/ - Сетевая штаб-квартира экспертов «Лаборатории Касперского»
12. https://moodle.osu.ru - Электронные курсы ОГУ в системе обучения moodle
13. https://openedu.ru/course/hse/DATPRO/ - «Открытое образование». Курсы, МООК: Защита информации.
14. https://ru.coursera.org/learn/metody-i-sredstva-zashity-informacii - «Coursera». Курсы, МООК: Методы и средства защиты информации
15. https://ru.coursera.org/learn/management-informacionnoi-bezopasnosti - «Coursera». Курсы, МООК: Менеджмент информационной безопасности
16. https://www.intuit.ru/studies/courses/3648/890/info – «Интуит. Национальный открытый университет». Курсы, МООК: Аттестация объектов информатизации по требованиям безопасности информации.
17. https://www.intuit.ru/studies/courses/3649/891/info – «Интуит. Национальный открытый университет». Курсы, МООК: Техническая защита информации. Организация защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

18. https://www.intuit.ru/studies/courses/2291/591/info – «Интуит. Национальный открытый университет». Курсы, МООК: Общие вопросы технической защиты информации

19. https://www.intuit.ru/studies/courses/3620/862/info – «Интуит. Национальный открытый университет». Курсы, МООК: Нормативно-методическое обеспечение технической защиты информации

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

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий компьютерный класс и лаборатория технической защиты информации

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

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.