

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 09:20:02

Уникальный программный ключ

fd935d10451b860e912264c0378f8448452b603f94388008e29877a6bcbf5

**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ»
«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»**

Факультет экономики, управления и юриспруденции

Кафедра «Управление и бизнес-информатика»

УТВЕРЖДАЮ

Проректор по учебно-методической работе

Г.П. Узунова / Г.П. Узунова

«02» февраля 2026 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации от утечки по техническим каналам

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника

Бакалавр

Для всех

форм обучения

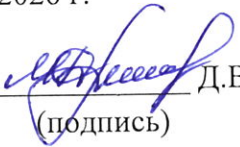
Симферополь, 2026

Рабочая программа составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность» профиль Безопасность компьютерных систем, утвержденным приказом Министерства образования и науки Российской Федерации от 17.11.2020 г. № 1427 (зарегистрировано в Министерстве юстиции РФ 18.02.2021 №62548) с изменениями и дополнениями.

Программу составил Фурин А.Д., преподаватель

Рабочая программа дисциплины «Защита информации от утечки по техническим каналам» утверждена на заседании кафедры «Управление и бизнес-информатика».

Протокол № 6 от 29.01.2026 г.

Заведующий кафедрой  Д.В. Моторина
(подпись)

Индекс дисциплины по учебному плану	Наименование дисциплины
Б1.О.11	ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ
Цель изучения дисциплины	Формирование компетенций, направленных на развитие научного мировоззрения, представления о современной картине мира, приобретение фундаментальных знаний и овладение основными приемами и методами познавательной деятельности как основой будущей профессиональной деятельности.
Место дисциплины в структуре ОПОП	Дисциплина относится к обязательной части блока 1. «Дисциплины (модули)» программы бакалавриата
Компетенции, формируемые в результате освоения дисциплины	ОПК-4, ОПК-11
Содержание дисциплины	Тема 1. Технические каналы утечки информации, обрабатываемой СВТ. Тема 2. Технические каналы утечки акустической речевой информации. Тема 3. Способы и средства защиты объектов информатизации от утечки информации по техническим каналам. Тема 4. Способы и средства защиты объектов информатизации от утечки информации, возникающей за счет наводок ПЭМИ. Тема 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 36 зачетных единиц (108 часов)
Форма промежуточной аттестации	Зачет/экзамен

Содержание

1. Цель и перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы бакалавриата	5
2. Место дисциплины в структуре ОПОП бакалавриата	5
3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся	5
4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	6
5. Контроль качества освоения дисциплины	6
6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	10
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.....	11
8. Методические указания для обучающихся по освоению дисциплины	12
9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)	12
10. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине	12
Приложение к РПД	13

1. Цель и перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы бакалавриата

Целью изучения дисциплины «Защита информации от утечки по техническим каналам» является формирование у обучающихся системы фундаментальных знаний о физических законах и явлениях природы, развитие научного мировоззрения и физического мышления, а также овладение методами научного познания и практическими навыками применения физических законов при решении профессиональных и прикладных задач.

В результате освоения ОПОП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ОПК-4	Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1. Применяет физические явления и эффекты для решения практических задач ОПК-4.2. Анализирует процессы, протекающие в линейных и нелинейных электрических цепях, с применением методов анализа в переходных и установившихся режимах в частотной и временной областях ОПК-4.3. Использует принципы работы элементов и функциональных узлов электронной аппаратуры при исследовании средств защиты информации
ОПК-11	Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.1. Проводит физический эксперимент, обрабатывает его результаты ОПК-11.2. Использует стандартные вероятностно-статистические методы анализа экспериментальных данных

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.О.24 «Защита информации от утечки по техническим каналам» относится к обязательной части блока 1. «Дисциплины (модули)» учебного плана ОПОП бакалавриата по направлению подготовки 10.03.02 «Информационная безопасность».

Дисциплина «Защита информации от утечки по техническим каналам» изучается обучающимися очной формы обучения в 5-6 семестрах, очно-заочной формы обучения – в 5-6 семестрах.

При изучении данной дисциплины обучающийся использует знания, умения и навыки, которые сформированы в процессе изучения предшествующих дисциплин: «высшая математика», «информационные технологии в профессиональной деятельности».

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 36 зачетных единицы (з. е.), 108 академических часов.

3.1. Объем дисциплины по видам учебных занятий (в часах)

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 8 зачётных единицы 288 часа

Объём дисциплины	Всего часов
Общая трудоёмкость дисциплины	108
Контактная работа	48
Аудиторная работа (всего):	48
Лекции	16
Семинары, практические занятия	32
Самостоятельная работа обучающихся (всего)	24
Зачет	+
Экзамен	36

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 8 зачётных единицы 288 часа

Объём дисциплины	Всего часов
Общая трудоёмкость дисциплины	108
Контактная работа	24
Аудиторная работа (всего):	24
Лекции	8
Семинары, практические занятия	16
Самостоятельная работа обучающихся (всего)	48
Зачет	+
Экзамен	36

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоёмкость по видам учебных занятий (в академических часах)

№ темы	Наименование темы	Всего		Количество часов					
		ОФО	ОЗФО	Контактная работа				Внеаудит. Работа	
				Лекции		Практические		Самост. Работа	
				ОФО	ОЗФО	ОФО	ОЗФО	ОФО	ОЗФО
1.	Технические каналы утечки информации, обрабатываемой СВТ.	16	16	2	2	6	2	4	8
2.	Технические каналы утечки акустической речевой информации.	14	14	2	2	6	2	4	8
3.	Способы и средства защиты объектов информатизации от утечки информации по техническим каналам.	14	14	2	2	6	2	4	8
4.	Способы и средства защиты объектов информатизации от	14	14	2	2	6	2	4	8

	утечки информации, возникающей за счет наводок ПЭМИ.								
5.	Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.	14	14	2	2	6	2	4	8
Всего по дисциплине		72	72	10	10	30	10	20	40
Зачет									
Экзамен		36	36						
Итого		108	108						

4.2 Содержание дисциплины (модуля), структурированное по разделам (темам)

Тема 1. Технические каналы утечки информации, обрабатываемой СВТ.

Защищаемая информация, источники информативных сигналов, среда распространения и возможная точка приема. Контролируемая зона. Этапы обследования помещения, описание оборудования и построение модели угроз.

Тема 2. Технические каналы утечки акустической речевой информации.

Возникновение и распространение речевого сигнала. Передача звука через ограждающие конструкции, двери, окна, вентиляцию и инженерные коммуникации. Звукоизоляция и звукопоглощение.

Тема 3. Способы и средства защиты объектов информатизации от утечки информации по техническим каналам.

Побочные электромагнитные излучения и наводки при работе технических средств. Влияние размещения оборудования, кабельных трасс, питания и заземления. Экранирование и рациональное размещение. Визуальное наблюдение экранов и документов, отражения и видеосъемка. Электроакустические преобразования во вспомогательных технических средствах и системах. Условия возникновения каналов.

Тема 4. Способы и средства защиты объектов информатизации от утечки информации, возникающей за счет наводок ПЭМИ.

Пассивные и активные меры. Выбор средств по результатам обследования: условия применения, учет, эксплуатация. Достоверность измерений и ограничения результатов контроля.

Тема 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.

Первичное и повторное обследование, проверка после ремонта и изменения конфигурации. Документирование результатов, выявление недостатков и корректирующих мер.

4.3. Темы практических занятий

Тема 1. Технические каналы утечки информации, обрабатываемой СВТ. (2 часа)
--

1. Определение потенциальных каналов для условного помещения. 2. Составление схемы контролируемой зоны. 3. Оформление перечня технических средств.
Тема 2. Технические каналы утечки акустической речевой информации. (2 часа) 1. Анализ путей распространения речи в переговорной. 2. Подбор мер защиты дверей и вентиляции. 3. Разбор протокола контрольной оценки.
Тема 3. Способы и средства защиты объектов информатизации от утечки информации по техническим каналам. (2 часа) 1. Инвентаризация рабочего места. 2. Анализ условий схемы кабельных трасс. 3. Составление плана обследования после переноса оборудования . 4. Сущность позиционирования товара.
Тема 4. Способы и средства защиты объектов информатизации от утечки информации, возникающей за счет наводок ПЭМИ. (2 часа) 1. Матрица «канал – источник – мера–проверка». 2. Сравнение вариантов защиты информации. 3. Оформление программы контрольных действий.
Тема 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам. (2 часа) 1. Итоговый кейс по переговорной и рабочему месту: перечень каналов, меры, график контроля, подведение итогов.

4.4. Содержание самостоятельной работы

Тема 1. Технические каналы утечки информации, обрабатываемой СВТ. (2 часа) 1. Определение потенциальных каналов для условного помещения. 2. Составление схемы контролируемой зоны. 3. Оформление перечня технических средств.
Тема 2. Технические каналы утечки акустической речевой информации. (2 часа) 1. Анализ путей распространения речи в переговорной. 2. Подбор мер защиты дверей и вентиляции.

3. Разбор протокола контрольной оценки.
Тема 3. Способы и средства защиты объектов информатизации от утечки информации по техническим каналам. (2 часа) 1. Инвентаризация рабочего места. 2. Анализ условий схемы кабельных трасс. 3. Составление плана обследования после переноса оборудования . 4. Сущность позиционирования товара.
Тема 4. Способы и средства защиты объектов информатизации от утечки информации, возникающей за счет наводок ПЭМИ. (2 часа) 1. Матрица «канал – источник – мера–проверка». 2. Сравнение вариантов защиты информации. 3. Оформление программы контрольный действий.
Тема 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам. (2 часа) 1. Итоговый кейс по переговорной и рабочему месту: перечень каналов, меры, график контроля, подведение итогов.

5. Контроль качества освоения дисциплины

Текущий контроль и промежуточная аттестация осуществляются в соответствии с «Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся в Автономной некоммерческой организации «Образовательная организация высшего образования» «Университет экономики и управления».

Вид промежуточной аттестации – зачет. Форма проведения промежуточной аттестации в целом по дисциплине – письменный зачет.

Оценочные средства по дисциплине приведены в Приложении к РПД.

6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная литература:

1. Хорев, П. Б. Программно-аппаратная защита информации : учебник и практикум для вузов / П. Б. Хорев. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 367 с. — ISBN 978-5-534-16542-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/535678> (дата обращения: 29.09.2026). — Режим доступа: для авторизир. пользователей.

2. Галицкий, А. В. Технологии безопасности информационно-вычислительных систем и сетей : учебное пособие / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. — Москва : Солон-Пресс, 2023. — 704 с. — ISBN 978-5-91359-524-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/130583.html> (дата обращения: 29.09.2026). — Режим доступа: для авторизир. пользователей.

3. Гришина, Н. В. Организация комплексной системы защиты информации : учебное пособие / Н. В. Гришина. — Москва : ФОРУМ : ИНФРА-М, 2022. — 256 с. — ISBN 978-5-00091-722-0. — Текст : электронный // Znanium.com : [сайт]. — URL: <https://znanium.com/catalog/product/1865456> (дата обращения: 29.09.2026). — Режим доступа: для авторизир. пользователей.

4. Мельников, В. П. Информационная безопасность и защита информации : учебник / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под редакцией С. А. Клейменова. — 8-е изд., стер. — Москва : Академия, 2023. — 336 с. — ISBN 978-5-4468-9876-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/140566.html> (дата обращения: 29.09.2026). — Режим доступа: для авторизир. пользователей.

5. Парошин, А. А. Нормативно-правовые основы защиты информации : учебное пособие / А. А. Парошин. — Владивосток : Дальневосточный федеральный университет, 2024. — 112 с. — ISBN 978-5-7444-5589-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/128415.html> (дата обращения: 29.09.2026). — Режим доступа: для авторизир. пользователей.

б) дополнительная литература:

6. Лукацкий, А. В. Обнаружение атак / А. В. Лукацкий. — 2-е изд. — Москва : ДМК Пресс, 2023. — 598 с. — ISBN 978-5-97060-987-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/146776.html> (дата обращения: 29.09.2026). — Режим доступа: для авторизир. пользователей.

7. Едомский, Д. Защита информации при реализации государственных информационных проектов / Д. Едомский // Администратор информационных технологий. — 2023. — № 9. — С. 76–78. — Текст : электронный. — URL: <https://www.meteorf.gov.ru/documents/21/10770/.^2>

8. Черкас, Ю. Защита от современных кибератак: мифы и реальность / Ю. Черкас // Администратор информационных технологий. — 2023. — № 9. — С. 40–43. — Текст : электронный. — URL: <https://www.meteorf.gov.ru/documents/21/10770/.^2>

9. Громов, И. Безопасность информации на государственном уровне / И. Громов // Администратор информационных технологий. — 2023. — № 9. — С. 20–24. — Текст : электронный. — URL: <https://www.meteorf.gov.ru/documents/21/10770/.^2>

10. Старостина, Е. Мишень социальной инженерии — это вы сами / Е. Старостина, Е. Хрусталева // Администратор информационных технологий. — 2023. — № 9. — С. 64–67. — Текст : электронный. — URL: <https://www.meteorf.gov.ru/documents/21/10770/.^2>

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. ФСТЭК России (Федеральная служба по техническому и экспортному контролю) : официальный сайт. — URL: <https://fstec.ru> — Текст : электронный.

2. ФСБ России (Центр защиты информации и специальной связи) : официальный сайт. — URL: <https://fsb.ru/fsb/supplement.htm> — Текст : электронный.

3. Министерство цифрового развития, связи и массовых коммуникаций РФ : официальный сайт. — URL: <https://digital.gov.ru> — Текст : электронный.

4. Реестр российского программного обеспечения : официальный сайт. — URL: <https://reestr.digital.gov.ru> — Текст : электронный.

5. Портал «Госуслуги» (раздел «Безопасность в сети») : официальный сайт. — URL: <https://www.gosuslugi.ru> — Текст : электронный.

6. Информационно-правовой портал «Гарант» : официальный сайт. — URL: <http://www.garant.ru> — Текст : электронный.

7. Цифровой образовательный ресурс «IPRsmart» : официальный сайт. — URL: <http://www.iprbookshop.ru> — Текст : электронный.

8. Научная электронная библиотека «КиберЛенинка» : официальный сайт. — URL: <https://cyberleninka.ru> — Текст : электронный.

8. Методические указания для обучающихся по освоению дисциплины

При проведении лекций, семинарских (практических) занятий, самостоятельной работе обучающихся применяются интерактивные формы проведения занятий с целью погружения обучающихся в реальную атмосферу профессионального сотрудничества по разрешению проблем, оптимальной выработки навыков и качеств будущего специалиста. Интерактивные формы проведения занятий предполагают обучение в сотрудничестве. Все участники образовательного процесса (преподаватель и обучающиеся) взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуацию.

В учебном процессе используются интерактивные формы занятий:

- творческое задание. Выполнение творческих заданий требует от обучающегося воспроизведение полученной ранее информации в форме, определяемой преподавателем, и требующей творческого подхода;
- групповое обсуждение. Групповое обсуждение кого-либо вопроса направлено на достижение лучшего взаимопонимания и способствует лучшему усвоению изучаемого материала.

В ходе освоения дисциплины при проведении контактных занятий используются следующие формы обучения, способствующие формированию компетенций: лекции-дискуссии; кейс-метод; решение задач; ситуационный анализ; обсуждение рефератов и докладов; разработка групповых проектов; встречи с представителями государственных и общественных организаций.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

В процессе лекционных и практических занятий используется следующее программное обеспечение:

- *программы, обеспечивающие доступ в сеть «Интернет» (например, «Google chrome»);
- *программы, демонстрации видео материалов (например, проигрыватель «Windows Media Player»);
- *программы для демонстрации и создания презентаций (например, «Microsoft PowerPoint»).

10. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине

Учебная аудитория

Оборудование учебной аудитории:

- рабочее место преподавателя ; посадочные места по количеству обучающихся ;
- доска классная;
- стенды информационные;

Учебно-наглядные пособия:

- ноутбук с лицензионным программным обеспечением и возможностью подключения к информационно-телекоммуникационной сети Интернет ;
- мультимедийная установка ;
- комплект учебно-наглядных пособий;

- комплект электронных видеоматериалов.

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.