

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 09:20:01

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

Основы проектирования защищенных инфокоммуникационных систем

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 Л. В. Яковенко, старший преподаватель

Рабочая программа дисциплины «Основы проектирования защищенных инфокоммуникационных систем» утверждена на заседании кафедры «Управление и бизнес-информатика».

Протокол № 6 от 29.01.2026 г.

Заведующий кафедрой  Д.В. Моторина
(подпись)

АННОТАЦИЯ	
Индекс дисциплины по учебному плану	Наименование дисциплины
Б1.В.ДВ.01.01	WEB-ДИЗАЙН
Цель изучения дисциплины	формирование у студентов профессиональных компетенций, необходимых для комплексного проектирования телекоммуникационных сетей и систем связи с одновременным обеспечением их информационной безопасности
Место дисциплины в структуре ОПОП	Дисциплина относится к «Дисциплинам по выбору 1» части, формируемой участниками образовательных отношений блока 1 программы бакалавриата
Компетенции, формируемые в результате освоения дисциплины	ПК-3
Содержание дисциплины	Тема 1. Системный подход к проектированию: разработка ТЗ и концепции защиты (ГОСТ 34-й серии). Тема 2. Проектирование структурированных кабельных систем (СКС) с учетом физической безопасности Тема 3. Эшелонированная защита сетевой инфраструктуры: проектирование DMZ и сегментация трафика. Тема 4. Обеспечение отказоустойчивости и катастрофоустойчивости защищенных систем. Тема 5. Интеграция средств криптографической защиты информации (СКЗИ) в каналы связи.
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часа)
Форма промежуточной аттестации	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	10
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	11
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

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

Цель изучения дисциплины «Основы проектирования защищенных инфокоммуникационных систем» – формирование у студентов профессиональных компетенций, необходимых для комплексного проектирования телекоммуникационных сетей и систем связи с одновременным обеспечением их информационной безопасности.

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

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ПК-3	Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-3.1. Знает методы и средства контроля эффективности технической защиты информации; ПК-3.2. Умеет контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; ПК-3.3. Владеет навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем, навыками участия в экспертизе состояния защищенности информации на объекте защиты

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Б1.В.ДВ.01.01 «Основы проектирования защищенных инфокоммуникационных систем» относится к части, формируемой участниками образовательных отношений блока 1 учебного плана ОПОП бакалавриата. Дисциплина «Основы проектирования защищенных инфокоммуникационных систем» изучается обучающимися очной формы обучения в 4 семестре, очно-заочной формы обучения – в 5 семестре.

При изучении данной дисциплины обучающийся использует знания, умения и навыки, которые сформированы в процессе изучения предшествующих дисциплин: «Информационные технологии в профессиональной деятельности», «Основы бизнес-информатики» и др.

Знания, умения и навыки, полученные при изучении дисциплины «Основы проектирования защищенных инфокоммуникационных систем», будут необходимы для углубленного и осмысленного восприятия дисциплин: «Безопасность беспроводных локальных сетей» и др.

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 4 зачетных единицы (з.е.), 144 академических часа.

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

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 4 зачётных единицы 144 часа

Объём дисциплины	Всего часов
Общая трудоёмкость дисциплины	144
Контактная работа	44
Аудиторная работа (всего):	44
Лекции	16
Семинары, практические занятия	28
Самостоятельная работа обучающихся (всего)	64
Экзамен	36

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 4 зачётных единицы 144 часа

Объём дисциплины	Всего часов
Общая трудоёмкость дисциплины	144
Контактная работа	34
Аудиторная работа (всего):	34
Лекции	12
Семинары, практические занятия	22
Самостоятельная работа обучающихся (всего)	74
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.	Тема 1. Системный подход к проектированию: разработка ТЗ и концепции защиты (ГОСТ 34-й серии).	20	20	2	2	2	2	16	16
2.	Тема 2. Проектирование структурированных кабельных систем (СКС) с учетом физической безопасности	20	20	4	2	2	2	14	16

3.	Тема 3. Эшелонированная защита сетевой инфраструктуры: проектирование DMZ и сегментация трафика.	24	24	4	4	12	10	8	10
4.	Тема 4. Обеспечение отказоустойчивости и катастрофоустойчивости защищенных систем.	24	24	4	2	8	6	12	16
5.	Тема 5. Интеграция средств криптографической защиты информации (СКЗИ) в каналы связи.	20	20	2	2	4	2	14	16
	Всего по дисциплине	108	108	16	12	28	22	64	74
	Контроль	36	36						
	Итого	144	144						

4.2. Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Системный подход к проектированию: разработка ТЗ и концепции защиты (ГОСТ 34-й серии) Раскрывается методология создания сложных систем согласно стандартам ГОСТ 34.601-90 и ГОСТ 34.602-89. Изучается процесс формирования модели угроз и нарушителя для конкретного объекта информатизации. Рассматривается структура технического задания (ТЗ): определение целей создания системы, классификация информации, требования к доступности и производительности каналов при условии наложения средств криптографической и технической защиты.

Тема 2. Проектирование структурированных кабельных систем (СКС) с учетом физической безопасности Изучаются инженерные аспекты построения фундамента сети. Рассматриваются стандарты ISO/IEC 11801 и TIA/EIA-568 применительно к защищенным объектам. Особое внимание уделяется правилам монтажа, исключающим несанкционированное подключение (например, обязательное использование экранированных коробов, скрытая прокладка трасс, контроль доступа к коммутационным шкафам и кроссовым помещениям).

Тема 3. Эшелонированная защита сетевой инфраструктуры: проектирование DMZ и сегментация трафика Анализируется архитектура безопасного периметра корпоративной сети. Раскрываются принципы зонирования: разделение публичного сегмента (DMZ — демилитаризованная зона), внутреннего сегмента пользователей и зоны управления оборудованием. Изучается микросегментация с помощью VLAN, списков контроля доступа (ACL) на маршрутизаторах и политик межсетевого экранирования для изоляции критических серверов.

Тема 4. Обеспечение отказоустойчивости и катастрофоустойчивости защищенных систем Рассматриваются методы обеспечения непрерывности бизнеса (Business Continuity). Изучается расчет коэффициента готовности (Availability) и проектирование резервирования на всех уровнях: дублирование каналов связи (протоколы LACP, STP/RSTP), кластеризация активного оборудования (HSRP/VRRP), организация резервных центров обработки данных (ЦОД) и зеркалирование информационных ресурсов.

Тема 5. Интеграция средств криптографической защиты информации (СКЗИ) в каналы связи Раскрываются вопросы безопасной передачи данных через недоверенные

среды (интернет, арендованные линии). Изучается проектирование виртуальных частных сетей (VPN) на базе протоколов IPsec и TLS. Анализируются требования к выбору криптоалгоритмов (в том числе отечественных по ГОСТ Р 34.12-2015), управлению ключами шифрования и обеспечению сквозной защиты каналов без деградации качества обслуживания (QoS).

4.3. Содержание практических занятий (очная форма обучения)

Тема 1. Системный подход к проектированию: разработка ТЗ и концепции защиты (ГОСТ 34-й серии) Раскрывается методология создания сложных систем согласно стандартам ГОСТ 34.601-90 и ГОСТ 34.602-89. Изучается процесс формирования модели угроз и нарушителя для конкретного объекта информатизации.
Тема 2. Проектирование структурированных кабельных систем (СКС) с учетом физической безопасности Изучаются инженерные аспекты построения фундамента сети. Рассматриваются стандарты ISO/IEC 11801 и TIA/EIA-568 применительно к защищенным объектам.
Тема 3. Эшелонированная защита сетевой инфраструктуры: проектирование DMZ и сегментация трафика Анализируется архитектура безопасного периметра корпоративной сети. Раскрываются принципы зонирования: разделение публичного сегмента (DMZ — демилитаризованная зона), внутреннего сегмента пользователей и зоны управления оборудованием.
Тема 4. Обеспечение отказоустойчивости и катастрофоустойчивости защищенных систем Рассматриваются методы обеспечения непрерывности бизнеса (<i>Business Continuity</i>). Изучается расчет коэффициента готовности (<i>Availability</i>) и проектирование резервирования на всех уровнях: дублирование каналов связи (протоколы LACP, STP/RSTP), кластеризация активного оборудования (HSRP/VRRP).
Тема 5. Интеграция средств криптографической защиты информации (СКЗИ) в каналы связи Раскрываются вопросы безопасной передачи данных через недоверенные среды (интернет, арендованные линии). Изучается проектирование виртуальных частных сетей (VPN) на базе протоколов IPsec и TLS.

4.4. Содержание самостоятельной работы

Тема 1. Системный подход к проектированию: разработка ТЗ и концепции защиты (ГОСТ 34-й серии) Структура технического задания (ТЗ): определение целей создания системы, классификация информации, требования к доступности и производительности каналов при условии наложения средств криптографической и технической защиты.
Тема 2. Проектирование структурированных кабельных систем (СКС) с учетом физической безопасности правила монтажа, исключающим несанкционированное подключение (например, обязательное использование экранированных коробов, скрытая прокладка трасс, контроль доступа к коммутационным шкафам и кроссовым помещениям).
Тема 3. Эшелонированная защита сетевой инфраструктуры: проектирование DMZ и сегментация трафика Микросегментация с помощью VLAN, списков контроля доступа (ACL) на маршрутизаторах и политик межсетевого экранирования для изоляции критических серверов.
Тема 4. Обеспечение отказоустойчивости и катастрофоустойчивости защищенных систем Организация резервных центров обработки данных (ЦОД) и зеркалирование информационных ресурсов.
Тема 5. Интеграция средств криптографической защиты информации (СКЗИ) в

каналы связи Требования к выбору криптоалгоритмов (в том числе отечественных по ГОСТ Р 34.12-2015), управлению ключами шифрования и обеспечению сквозной защиты каналов без деградации качества обслуживания (QoS).

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 – экзамен. Форма проведения промежуточной аттестации – письменный экзамен.

Фонд оценочных средств по дисциплине приведен в приложении к РПД.

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

а) основная

1. Башмакова, Е. И. Информатика и информационные технологии. Технология работы в MS WORD 2016 : учебное пособие / Е. И. Башмакова. — Москва : Ай Пи Ар Медиа, 2020. — 90 с. — ISBN 978-5-4497-0515-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/94204.html> (дата обращения: 16.01.2026). — Режим доступа: для авторизир. пользователей.

2. Фот, Ю. Д. Анализ уязвимостей и защита программного обеспечения : практикум / Ю. Д. Фот, Е. И. Ларионова. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2025. — 141 с. — ISBN 978-5-7410-3391-3. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/153174/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

б) дополнительная

3. Новиков, С. Н. Проектирование защищённых телекоммуникационных систем : учебное пособие / С. Н. Новиков, Г. В. Попков. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2018. — 439 с. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/102152/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

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

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

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

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

4. Российский интернет-портал и аналитическое агентство TAdviser: официальный сайт. — URL: <https://www.tadviser.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, «Microsoft Edge», «Google Chrome»);

- *программы, демонстрации видео материалов (например, проигрыватель «Windows Media Player»);

- *текстовые редакторы и процессоры (например, «Блокнот», «Microsoft Office Word»);

- *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: компьютеры с лицензионным программным обеспечением и возможностью подключения к информационно-телекоммуникационной сети Интернет ; мультимедийная установка.

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