

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 50.09.2026 09:20:02

Уникальный программный ключ:

fd935d10451b860e912264c037858448452bfdb603f94388008e29877a6bcbf5

**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

«02» февраля 2026 г.

Рабочая программа дисциплины

Криптографические методы защиты информации

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника

Бакалавр

Для всех

форм обучения

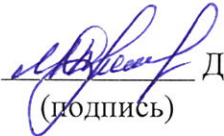
Симферополь, 2026

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 «Криптографические методы защиты информации» 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.О.29	КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
Цель изучения дисциплины	сформировать знания в области информационных технологий, выработать необходимые умения и навыки использования современных аппаратных и программных средств сбора, представления, хранения, передачи, обработки, анализа данных в профессиональной деятельности.
Место дисциплины в структуре ОПОП	Дисциплина «Криптографические методы защиты информации» является дисциплиной базовой части программы учебного плана и изучается на 2 курсе в III семестре очной формы обучения.
Компетенции, формируемые в результате освоения дисциплины	ОПК-49
Содержание дисциплины	Тема 1. Программно-аппаратные средства информационных систем Тема 2. Аппаратная организация управляющих компьютерных систем. Тема 3. Взаимодействие промышленных систем управления
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 5 зачетные единицы (180 часов)
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	11
6. Учебно-методическое обеспечение дисциплины	11
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	11
8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	12
9. Методические указания для обучающихся по освоению дисциплины	13
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)	13
11. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине	14
Приложение к РПД	15

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

Цель изучения дисциплины «Криптографические методы защиты информации» – сформировать знания в области информационных технологий, выработать необходимые умения и навыки использования современных аппаратных и программных средств сбора, представления, хранения, передачи, обработки, анализа данных в профессиональной деятельности.

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

Код компетенции	Результаты освоения ОПОП (содержание компетенций)	Планируемые результаты освоения дисциплины
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1. Использует типовые криптографические средства защиты информации, в том числе средства электронной подписи ОПК-9.2. Применяет методы и средства технической защиты информации для решения задач профессиональной деятельности

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина «Криптографические методы защиты информации» является дисциплиной базовой части программы учебного плана и изучается на 3 курсе в VI семестре очной формы обучения.

Для изучения дисциплины студент должен:

- знать основы дискретной математики и теории вероятности;
- знать теоретические основы современной криптографии,
- уметь пользоваться базовым программным и математическим обеспечением.

Для успешного освоения дисциплины «Криптографические методы защиты информации» студент должен изучить курсы «Дискретной математики» и «Теоретических основ криптографии».

Дисциплина «Теоретические основы криптографии» необходима в качестве предшествующей для дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем».

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 8 зачетных единицы (з.е.), 180 академических часа.

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

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 8 зачётных единицы 180 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	180
Контактная работа	52
Аудиторная работа (всего):	52
Лекции	18
Семинары, практические занятия	34
Самостоятельная работа обучающихся (всего)	92
Экзамен	36

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 5 зачётных единицы 180 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	180
Контактная работа	40
Аудиторная работа (всего):	40
Лекции	20
Семинары, практические занятия	20
Самостоятельная работа обучающихся (всего)	104
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 трудоемкость 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.	Введение	34	34	2	2	4	2	28	30
2.	Основы криптографических методов	34	34	4	2	4	2	28	30
3.	Методы и применение двухключевой криптографии	34	34	4	2	4	2	28	30
4	Симметричные шифры	34	32	4	1	4	1	28	30
5	Управление криптографическими ключами	32	32	4	1	4	1	28	30
6	Специальные криптографические методы	36	30	6	2	6	2	24	26
		144	144	18	20	34	20	92	104

	Контроль	36	36						
	Итого	180	180						

4.2. Содержание дисциплины, структурированное по темам (разделам)

Введение.

Предмет и задачи дисциплины. Рекомендуемая литература. Краткий обзор проблематики и методов современной криптографии.

Тема 1. Основы криптографических методов

Основные используемые результаты теории чисел. Модель криптосистемы. Задачи и фундаментальные проблемы криптографии. Криптографический протокол как распределенный вычислительный алгоритм.

Тема 2. Методы и применение двухключевой криптографии.

Проблема неотказуемости от электронных сообщений и документов. Электронная цифровая подпись (ЭЦП) на основе сложности задачи дискретного логарифмирования по простому модулю. Криптосистемы RSA, Рабина, Шнорра, Эль-Гамала. Стандарты ЭЦП. Проблема анонимности пользователей. Схемы слепой подписи.

Тема 3. Симметричные шифры

Основные типы симметричных шифров и поточные шифры. Основные схемы построения блочных шифров, режимы использования и требования к ним. Стандарты симметричного шифрования AES и ГОСТ. Технология многоуровневого шифрования. Скоростные программные шифры. Схемы построения хэш-функций на основе блочных шифров.

Тема 4 Управление криптографическими ключами

Основные задачи и функции управления ключами. Иерархия ключевой системы. Инфраструктура открытых ключей. Цифровые сертификаты. Схемы разделения секрета, на основе китайской теоремы об остатках и на основе восстановления многочленов.

Тема 5 Специальные криптографические методы

Отрицаемое шифрование как

Метод защиты от атак с принуждением. Отрицаемое шифрование по открытому и разделяемому секретному ключу. Криптографические обманные ловушки. Методы обеспечения заданного уровня стойкости протокола криптографической защиты информации при использовании разделяемых секретных ключей малого размера

4.3. Содержание практических занятий (очная форма обучения)

Тема 2. Основы криптографических методов

Лабораторная работа №01.

«Генерация значений заданного порядка по простому модулю»

Лабораторная работа №02.

«Управление входным и выходным потоками устройств»

Лабораторная работа №03.

«Реализация работы вакуумного перегонного куба»

Лабораторная работа №04.

«Реализация работы ректификационной колонны»

Тема 3. Методы и применение двухключевой криптографии.

Лабораторная работа №05.

«Схема разделения секрета между несколькими хранителями секрета»

Лабораторная работа №06.

«Пороговая схема разделения секрета на основе китайской теоремы об остатках»

Лабораторная работа №07. «Пороговая схема разделения секрета на основе механизма восстановления многочлена, заданного над конечным полем»
Тема 4 Симметричные шифры Лабораторная работа №08 Разработка режимов использования блочных шифров. Лабораторная работа №09. Экспоненциальный, коммутативный шифр. Лабораторная работа №10 Протокол бесключевого шифрования
Тема 5 Управление криптографическими ключами Лабораторная работа №11. Схема разделения секрета между несколькими хранителями секрета. Лабораторная работа №12. Пороговая схема разделения секрета на основе китайской теоремы об остатках Лабораторная работа №13. Пороговая схема разделения секрета на основе механизма восстановления многочлена, заданного над конечным полем.

4.4. Содержание самостоятельной работы

№ п/п	Вид самостоятельной работы	Наименование работы и содержание
1	Курсовая работа	Построение алгоритма шифрования, электронной цифровой подписи, включая разработку компьютерной программы.
2	Самостоятельное изучение онлайн-курса	Онлайн-курс «Криптографические методы защиты информации» https://farvater.gumrf.ru/course/view.php?id=3372

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.

а) основная литература:

1. Александрова, Е. Б. Криптографические методы защиты информации. Элементы алгебраической геометрии : учебное пособие / Е. Б. Александрова, А. В. Ярмак. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2023. — 106 с. — ISBN 978-5-7422-8017-0. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/143094/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей.

2. Кочкуров, Л. А. Криптографические алгоритмы, модели и методы обеспечения информационной безопасности : учебное пособие / Л. А. Кочкуров, Н. Ю. Хороводова, Д.

В. Кондратов. — Саратов : Саратовский государственный технический университет имени Ю.А. Гагарина, ЭБС АСВ, 2026. — 136 с. — ISBN 978-5-7433-3700-2. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/161450/details> (дата обращения: 27.01.2026). — DOI: <https://doi.org/10.23682/161450>. — Режим доступа: для авторизир. пользователей

б) дополнительная литература:

3. Швечкова, О. Г. Базовые криптографические алгоритмы защиты информации : учебное пособие / О. Г. Швечкова, А. Н. Пылькин, Д. В. Марчев. — Москва : КУРС, 2024. — 168 с. — ISBN 978-5-906923-83-7. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/144772/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, «Microsoft Office Word»);
- *табличные процессоры (например, «Microsoft Office Excel»);
- *системы управления базами данных (например, «Microsoft Office Access»);
- *программы для демонстрации и создания презентаций (например, «Microsoft PowerPoint»);
- *проблемно-ориентированные пакеты прикладных программ по отраслям и сферам деятельности (например, «1С: Управление нашей фирмой», «Loginom Community Edition»).

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.