

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:

fd935d10451b860e912264c037858448452bfdb603f947889008e29877a6bcbf5

**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

Методы и средства криптографической защиты информации

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника

Бакалавр

Для всех

форм обучения

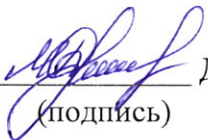
Симферополь, 2026

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 старший преподаватель Яковенко Л.В.

Рабочая программа дисциплины «Методы и средства криптографической 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.25	Методы и средства криптографической защиты информации
Цель изучения дисциплины	формирование у студентов фундаментальных знаний в области классической и современной криптографии, а также устойчивых практических навыков применения математических методов для обеспечения конфиденциальности, целостности и подлинности данных
Место дисциплины в структуре ОПОП	Дисциплина Методы и средства криптографической защиты информации относится к базовой части ОПОП и является обязательной для освоения.
Компетенции, формируемые в результате освоения дисциплины	ОПК-9
Содержание дисциплины	Тема 1. Симметричные криптосистемы: блочные шифры и стандарты ГОСТ Тема 2. Асимметричная криптография: алгоритм RSA и протокол Диффи-Хеллмана Тема 3. Хеш-функции и коды аутентификации сообщений (MAC) Тема 4. Электронная подпись: российский стандарт ГОСТ Р 34.10-2012 Тема 5. Инфраструктуры открытых ключей (PKI) и управление жизненным циклом сертификатов Тема 6. Протоколы безопасности транспортного уровня: архитектура TLS 1.3
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часов)
Форма промежуточной аттестации	Зачет

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. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	11
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	12
8. Методические указания для обучающихся по освоению дисциплины	13
9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)	13
10. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине	14

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

Целью преподавания дисциплины «Методы и средства криптографической защиты информации» является формирование у студентов фундаментальных знаний в области классической и современной криптографии, а также устойчивых практических навыков применения математических методов для обеспечения конфиденциальности, целостности и подлинности данных.

Основная задача состоит в том, чтобы студенты освоили принципы комплексного подхода к вопросам безопасности, научились анализировать потенциальные угрозы и выявлять риски безопасности, а также познакомились с современными методами и средствами защиты информации в компьютерных сетях.

Кроме того, дисциплина направлена на ознакомление студентов с основными положениями нормативно-правовой базы в области информационной безопасности, такими как требования к защите корпоративных информационных систем от несанкционированного доступа, скрытых воздействий и утечек информации по техническим каналам.

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-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности соответствующих проектных решений	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 Методы и средства криптографической защиты информации относится к базовой части ОПОП и является обязательной для освоения, изучается обучающимися очной формы обучения в 5 семестре, очно-заочной формы обучения – в 5 семестре.

Дисциплина является базовой для освоения дисциплин Криптографические протоколы.

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)	100
Курсовая работа	-
Зачет	+

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 4 зачётных единицы 144 часа

Объём дисциплины	Всего часов
Общая трудоёмкость дисциплины	144
Контактная работа	28
Аудиторная работа (всего):	28
Лекции	10
Семинары, практические занятия	18
Самостоятельная работа обучающихся (всего)	116
Курсовая работа	-
Зачет	+

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. Симметричные криптосистемы: блочные шифры и стандарты ГОСТ	28	26	4	2	6	4	18	20
2.	Тема 2. Асимметричная криптография: алгоритм RSA и протокол Диффи-Хеллмана	28	26	4	2	6	4	18	20

3.	Тема 3. Хеш-функции и коды аутентификации сообщений (MAC)	22	26	2	2	4	4	16	20
4.	Тема 4. Электронная подпись: российский стандарт ГОСТ Р 34.10-2012	22	24	2	2	4	2	16	20
5.	Тема 5. Инфраструктуры открытых ключей (PKI) и управление жизненным циклом сертификатов	22	21	2	1	4	2	16	18
6.	Тема 6. Протоколы безопасности транспортного уровня: архитектура TLS 1.3	22	21	2	1	4	2	16	18
	Всего по дисциплине	144	144	16	10	28	18	100	116
	Контроль	-	-						
	Итого	144	144						

4.2. Содержание дисциплины, структурированное по темам (разделам)

Разделы, темы, дидактические единицы
Тема 1. Симметричные криптосистемы: блочные шифры и стандарты ГОСТ Раскрывается принцип работы алгоритмов, использующих один и тот же секретный ключ для зашифрования и расшифрования. Подробно анализируются современные российские стандарты: <i>ГОСТ 34.12-2015 «Мagma»</i> — блочный шифр с длиной блока 64 бита (наследник советского стандарта), сохраняемый для совместимости со старыми системами. <i>ГОСТ 34.12-2015 «Кузнечик»</i> — современный блочный шифр с длиной блока 128 бит, построенный на основе подстановочно-перестановочных сетей (SPN). Рассматриваются режимы их работы (ECB, CBC, CFB, OFB, CTR) и то, как выбор режима влияет на распространение ошибок и возможность параллельных вычислений.
Тема 2. Асимметричная криптография: алгоритм RSA и протокол Диффи-Хеллмана Изучается концепция использования ключевой пары: открытого ключа (для зашифрования или проверки подписи) и закрытого ключа (для расшифрования или создания подписи). Алгоритм RSA. Раскрывается его математическая основа (сложность задачи факторизации больших целых чисел), процесс генерации ключей, а также схемы дополнения данных (PKCS#1 v1.5, OAEP) для защиты от атак на детерминированное шифрование. Рассматривается протокол Диффи-Хеллмана выработки общего секретного ключа по незащищенному каналу связи, который лег в основу современных протоколов обмена ключами (TLS Handshake).
Тема 3. Хеш-функции и коды аутентификации сообщений (MAC) Раскрываются методы обеспечения целостности и подлинности данных без обязательного сохранения их тайны. Изучаются отечественный стандарт <i>ГОСТ Р 34.11-2012 «Стрибог»</i> (с длинами хеш-кода 256 и 512 бит) и международный стандарт SHA-3. Анализируется структура Меркла-Дамгора и губчатой конструкции (sponge construction). Отдельно рассматривается механизм HMAC (ключевого хеширования), который объединяет хеш-функцию с симметричным ключом для создания имитовставки, гарантирующей, что сообщение не было изменено и отправлено доверенным лицом.
Тема 4. Электронная подпись: российский стандарт ГОСТ Р 34.10-2012 Детально разбирается технология юридически значимой электронной подписи. Описывается схема на базе асимметричного криптоалгоритма и хеш-функции: автор сообщения подписывает своим закрытым

ключом хеш-код документа, а любой желающий может проверить подпись открытым ключом автора. Сравниваются подходы к подписи через задачу дискретного логарифмирования и на эллиптических кривых (*ECC*), где при равной стойкости используются ключи значительно меньшей длины, что критично для мобильных устройств и смарт-карт.

Тема 5. Инфраструктуры открытых ключей (PKI) и управление жизненным циклом сертификатов Криптографические алгоритмы бесполезны без доверия к открытому ключу. Тема раскрывает архитектуру *PKI* как системы, связывающей открытые ключи с личностью владельца через цифровые сертификаты *X.509*. Рассматриваются роли удостоверяющих центров (*CA*), процессы регистрации, выдачи, обновления, приостановки действия и отзыва сертификатов (через списки отзыва *CRL* и протокол *OCSP*). Практический аспект включает работу с российскими средствами криптографической защиты информации (*СКЗИ*), такими как КриптоПро CSP, для интеграции подписи в документооборот.

Тема 6. Протоколы безопасности транспортного уровня: архитектура TLS 1.3 Анализируется наиболее массовое применение криптографии — защита веб-трафика. Раскрывается устройство протокола *TLS (Transport Layer Security* версии 1.3). Описываются этапы установления защищенного соединения: подтверждение владения доменом, анонимный или аутентифицированный обмен ключами (на базе алгоритма Диффи-Хеллмана на эллиптических кривых для обеспечения совершенной прямой секретности — *PFS*), согласование набора алгоритмов (*AEAD-суиты*, объединяющие шифр и код аутентификации). Подчеркивается отказ от уязвимых старых алгоритмов (*RC4, MD5*, статических ключей *RSA*) в пользу современной криптографии.

4.3. Содержание практических занятий (очная форма обучения)

Разделы, темы, дидактические единицы
Тема 1. Симметричные криптосистемы: блочные шифры и стандарты ГОСТ Раскрывается принцип работы алгоритмов, использующих один и тот же секретный ключ для зашифрования и расшифрования. Подробно анализируются современные российские стандарты: <i>ГОСТ 34.12-2015 «Мagma»</i> — блочный шифр с длиной блока 64 бита (наследник советского стандарта), сохраняемый для совместимости со старыми системами. <i>ГОСТ 34.12-2015 «Кузнечик»</i> — современный блочный шифр с длиной блока 128 бит, построенный на основе подстановочно-перестановочных сетей (<i>SPN</i>).
Тема 2. Асимметричная криптография: алгоритм RSA и протокол Диффи-Хеллмана Изучается концепция использования ключевой пары: открытого ключа (для зашифрования или проверки подписи) и закрытого ключа (для расшифрования или создания подписи). Алгоритм <i>RSA</i>. Раскрывается его математическая основа (сложность задачи факторизации больших целых чисел), процесс генерации ключей, а также схемы дополнения данных (<i>PKCS#1 v1.5, OAEP</i>) для защиты от атак на детерминированное шифрование.
Тема 3. Хеш-функции и коды аутентификации сообщений (MAC) Раскрываются методы обеспечения целостности и подлинности данных без обязательного сохранения их тайны. Изучаются отечественный стандарт <i>ГОСТ Р 34.11-2012 «Стрибог»</i> (с длинами хеш-кода 256 и 512 бит) и международный стандарт <i>SHA-3</i>. Анализируется структура Меркла-Дамгора и губчатой конструкции (<i>sponge construction</i>).
Тема 4. Электронная подпись: российский стандарт ГОСТ Р 34.10-2012 Детально разбирается технология юридически значимой электронной подписи. Описывается схема на базе асимметричного криптоалгоритма и хеш-функции: автор сообщения подписывает своим закрытым ключом хеш-код документа, а любой желающий может проверить подпись открытым ключом автора.

Тема 5. Инфраструктуры открытых ключей (PKI) и управление жизненным циклом сертификатов Криптографические алгоритмы бесполезны без доверия к открытому ключу. Тема раскрывает архитектуру PKI как системы, связывающей открытые ключи с личностью владельца через цифровые сертификаты X.509. Рассматриваются роли удостоверяющих центров (CA), процессы регистрации, выдачи, обновления, приостановки действия и отзыва сертификатов (через списки отзыва CRL и протокол OCSP).

Тема 6. Протоколы безопасности транспортного уровня: архитектура TLS 1.3 Анализируется наиболее массовое применение криптографии — защита веб-трафика. Раскрывается устройство протокола TLS (Transport Layer Security версии 1.3).

4.4. Содержание самостоятельной работы

Разделы, темы, дидактические единицы
Тема 1. Симметричные криптосистемы: блочные шифры и стандарты ГОСТ Рассматриваются режимы их работы (<i>ECB, CBC, CFB, OFB, CTR</i>) и то, как выбор режима влияет на распространение ошибок и возможность параллельных вычислений.
Тема 2. Асимметричная криптография: алгоритм RSA и протокол Диффи-Хеллмана Рассматривается протокол Диффи-Хеллмана выработки общего секретного ключа по незащищенному каналу связи, который лег в основу современных протоколов обмена ключами (<i>TLS Handshake</i>).
Тема 3. Хеш-функции и коды аутентификации сообщений (MAC) Механизм HMAC (ключевого хеширования), который объединяет хеш-функцию с симметричным ключом для создания имитовставки, гарантирующей, что сообщение не было изменено и отправлено доверенным лицом.
Тема 4. Электронная подпись: российский стандарт ГОСТ Р 34.10-2012 Подходы к подписи через задачу дискретного логарифмирования и на эллиптических кривых (<i>ECC</i>), где при равной стойкости используются ключи значительно меньшей длины, что критично для мобильных устройств и смарт-карт.
Тема 5. Инфраструктуры открытых ключей (PKI) и управление жизненным циклом сертификатов Практический аспект включает работу с российскими средствами криптографической защиты информации (СКЗИ), такими как КриптоПро CSP, для интеграции подписи в документооборот.
Тема 6. Протоколы безопасности транспортного уровня: архитектура TLS 1.3 Этапы установления защищенного соединения: подтверждение владения доменом, анонимный или аутентифицированный обмен ключами (на базе алгоритма Диффи-Хеллмана на эллиптических кривых для обеспечения совершенной прямой секретности — <i>PFS</i>), согласование набора алгоритмов (<i>AEAD-суиты</i>, объединяющие шифр и код аутентификации). Подчеркивается отказ от уязвимых старых алгоритмов (<i>RC4, MD5</i>, статических ключей <i>RSA</i>) в пользу современной криптографии.

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 – письменный зачет.

Фонд оценочных средств по дисциплине приведен в приложении к РПД.

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

а) основная литература:

1. 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

2. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 3-е изд. — Саратов : Профобразование, 2024. — 543 с. — ISBN 978-5-4488-0074-0. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/145909/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

б) дополнительная литература:

3. Куликов, С. С. Информационная безопасность локальных компьютерных сетей : практикум / С. С. Куликов. — Воронеж : Воронежский государственный технический университет, ЭБС АСВ, 2021. — 57 с. — ISBN 978-5-7731-0969-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/118614.html> (дата обращения: 01.04.2025). — Режим доступа: для авторизир. пользователей

4. Урбанович, П. П. Компьютерные сети : учебное пособие / П. П. Урбанович, Д. М. Романенко. — Москва, Вологда : Инфра-Инженерия, 2022. — 460 с. — ISBN 978-5-9729-0962-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/124197.html> (дата обращения: 01.07.2025). — 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 учебного кабинета:

- 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.

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