

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:

fd935d10451b860e912264c037858448453b603f94388008c29877a6bcbf5

**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

Криптографические протоколы

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника

Бакалавр

Для всех

форм обучения

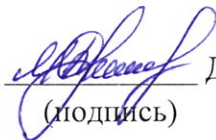
Симферополь, 2026

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 «Криптографические протоколы» 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.30	Криптографические протоколы
Цель изучения дисциплины	изучение студентами принципов построения, методов формального анализа стойкости и особенностей практической реализации сложных криптосистем, обеспечивающих безопасный обмен сообщениями между участниками электронного взаимодействия
Место дисциплины в структуре ОПОП	Дисциплина Криптографические протоколы относится к базовой части ОПОП и является обязательной для освоения.
Компетенции, формируемые в результате освоения дисциплины	ОПК-9
Содержание дисциплины	Тема 1. Основы теории криптографических протоколов: классификация, свойства и формальные модели. Тема 2. Протоколы идентификации и строгой аутентификации сторон. Тема 3. Протоколы распределения ключей: Диффи-Хеллмана и Керберос. Тема 4. Построение защищенных каналов связи: TLS 1.3 и IPsec. Тема 5. Схемы электронной подписи и протоколы неоспоримости (Non-repudiation). Тема 6. Атаки на криптографические протоколы и методы их анализа.
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часов)
Форма промежуточной аттестации	Зачет с оценкой

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 «Криптографические протоколы» является изучение студентами принципов построения, методов формального анализа стойкости и особенностей практической реализации сложных криптосистем, обеспечивающих безопасный обмен сообщениями между участниками электронного взаимодействия.

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 Криптографические протоколы 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 Защита операционных систем сетевых устройств.

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 с оценкой	+

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 с оценкой	+

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. Основы теории криптографических протоколов: классификация, свойства и формальные модели.	28	26	4	2	6	4	18	20
2.	Тема 2. Протоколы идентификации и строгой аутентификации сторон.	28	26	4	2	6	4	18	20

3.	Тема 3. Протоколы распределения ключей: Диффи-Хеллмана и Керберос.	22	26	2	2	4	4	16	20
4.	Тема 4. Построение защищенных каналов связи: TLS 1.3 и IPsec.	22	24	2	2	4	2	16	20
5.	Тема 5. Схемы электронной подписи и протоколы неоспоримости (Non-repudiation).	22	21	2	1	4	2	16	18
6.	Тема 6. Атаки на криптографические протоколы и методы их анализа.	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)

Тема 1. Основы теории криптографических протоколов: классификация, свойства и формальные модели Раскрывается понятие протокола как распределенного алгоритма взаимодействия участников в недоверенной среде. Изучаются фундаментальные требования к протоколам (однозначность толкования шагов, полнота описания реакций на любые ситуации). Рассматриваются основные классы протоколов по целевому назначению: аутентификационные, протоколы обмена ключами, протоколы голосования и подписания контрактов. Вводятся формальные методы описания и верификации с использованием BAN-логики (Logic of Beliefs), позволяющей математически доказать отсутствие логических ошибок в последовательности обмена сообщениями.

Тема 2. Протоколы идентификации и строгой аутентификации сторон Детально анализируются механизмы подтверждения подлинности субъектов. Раскрывается разница между односторонней и взаимной (*mutual*) аутентификацией. Изучается уязвимость простых схем к атаке повторной передачи (*replay attack*) и способы защиты от нее через использование одноразовых чисел (*nonce*) и меток времени (*timestamps*). Практическая часть посвящена разбору механизмов CHAP (Challenge Handshake Authentication Protocol) и протоколов на основе симметричного шифрования (*Needham-Schroeder Shared-Key Protocol*), а также их модификаций для устранения известных недостатков.

Тема 3. Протоколы распределения ключей: Диффи-Хеллмана и Керберос Рассматриваются методы безопасного получения общего секретного ключа по открытому каналу связи. Подробно разбирается классическая схема Диффи-Хеллмана (*Diffie-Hellman Key Exchange*), ее математическая основа (задача дискретного логарифмирования) и главная слабость — атака «человек посередине» (*MitM*). Изучаются модификации с использованием цифровых сертификатов для аутентификации сторон. Анализируется архитектура сети доверия Kerberos как централизованной системы выдачи сеансовых билетов (*TGS/AS*). Описывается процесс получения билета на получение билетов (*TGT*) и последующего доступа к сервису, включая защиту от перехвата паролей и повторного использования билетов.

Тема 4. Построение защищенных каналов связи: TLS 1.3 и IPsec Изучается применение криптографических протоколов для обеспечения конфиденциальности и целостности всего потока данных. Для транспортного уровня (*TLS 1.3*) раскрывается

современный handshake-процесс: переход исключительно на эфемерный обмен ключами Диффи-Хеллмана (*ECDHE*) для обеспечения совершенной прямой секретности (*PFS*), отказ от слабых алгоритмов и сжатие процесса установления соединения до одного кругового обхода (*RTT*). Для сетевого уровня (*IPsec*) рассматриваются архитектуры *AH* (*Authentication Header*) и *ESP* (*Encapsulating Security Payload*), режимы работы (*транспортный* и *туннельный*), а также протокол автоматического управления ключами *IKEv2*.

Тема 5. Схемы электронной подписи и протоколы неоспоримости (Non-repudiation)

Анализируются протоколы, решающие задачу доказательства авторства сообщения третьей стороне (арбитру). Разбираются стандарты цифровой подписи (*ГОСТ Р 34.10-2012*, *RSA-PSS*, *ECDSA*). Особое внимание уделяется защите от атак на подмену подписанных фрагментов и необходимости использования детерминированных функций хеширования. Вводится концепция службы доверенного времени (*Timestamping Authority - TSA*) и квитанций о доставке (*Delivery Receipt*), которые необходимы для реализации свойства неотрекаемости в системах электронного документооборота согласно стандартам типа *CAdES/XAdES*.

Тема 6. Атаки на криптографические протоколы и методы их анализа

Тема систематизирует угрозы безопасности именно на уровне логики протокола, а не криптоанализа отдельных алгоритмов. Раскрываются следующие виды атак: Атака отражения (*Reflection attack*): когда злоумышленник заставляет жертву расшифровать собственное сообщение своим же ключом. Атака на тип сообщения (*Type confusion*): подмена смысла поля из-за отсутствия жесткой типизации данных в потоке. Атаки на побочные каналы (*Side-channel attacks*): извлечение ключей через измерение времени выполнения операций или потребления энергии. Для противодействия изучаются инструменты формальной проверки моделей (*ProVerif*, *Scyther*), позволяющие автоматически найти сценарии атак на описанную спецификацию протокола..

4.3. Содержание практических занятий (очная форма обучения)

Разделы, темы, дидактические единицы
Тема 1. Основы теории криптографических протоколов: классификация, свойства и формальные модели Раскрывается понятие протокола как распределенного алгоритма взаимодействия участников в недоверенной среде. Изучаются фундаментальные требования к протоколам (однозначность толкования шагов, полнота описания реакций на любые ситуации). Рассматриваются основные классы протоколов по целевому назначению: аутентификационные, протоколы обмена ключами, протоколы голосования и подписания контрактов.
Тема 2. Протоколы идентификации и строгой аутентификации сторон Детально анализируются механизмы подтверждения подлинности субъектов. Раскрывается разница между односторонней и взаимной (<i>mutual</i>) аутентификацией. Изучается уязвимость простых схем к атаке повторной передачи (<i>replay attack</i>) и способы защиты от нее через использование одноразовых чисел (<i>nonce</i>) и меток времени (<i>timestamps</i>).
Тема 3. Протоколы распределения ключей: Диффи-Хеллмана и Керберос Рассматриваются методы безопасного получения общего секретного ключа по открытому каналу связи. Подробно разбирается классическая схема Диффи-Хеллмана (<i>Diffie-Hellman Key Exchange</i>), ее математическая основа (задача дискретного логарифмирования) и главная слабость — атака «человек посередине» (<i>MitM</i>). Изучаются модификации с использованием цифровых сертификатов для аутентификации сторон. Анализируется архитектура сети доверия Kerberos как централизованной системы выдачи сеансовых билетов (<i>TGS/AS</i>).
Тема 4. Построение защищенных каналов связи: TLS 1.3 и IPsec Изучается применение

криптографических протоколов для обеспечения конфиденциальности и целостности всего потока данных. Для транспортного уровня (*TLS 1.3*) раскрывается современный handshake-процесс: переход исключительно на эфемерный обмен ключами Диффи-Хеллмана (*ECDHE*) для обеспечения совершенной прямой секретности (*PFS*), отказ от слабых алгоритмов и сжатие процесса установления соединения до одного кругового обхода (*RTT*).

Тема 5. Схемы электронной подписи и протоколы неоспоримости (Non-repudiation)

Анализируются протоколы, решающие задачу доказательства авторства сообщения третьей стороне (арбитру). Разбираются стандарты цифровой подписи (*ГОСТ Р 34.10-2012*, *RSA-PSS*, *ECDSA*). Особое внимание уделяется защите от атак на подмену подписанных фрагментов и необходимости использования детерминированных функций хеширования.

Тема 6. Атаки на криптографические протоколы и методы их анализа

Тема систематизирует угрозы безопасности именно на уровне логики протокола, а не криптоанализа отдельных алгоритмов. Раскрываются следующие виды атак: Атака отражения (*Reflection attack*): когда злоумышленник заставляет жертву расшифровать собственное сообщение своим же ключом. Атака на тип сообщения (*Type confusion*): подмена смысла поля из-за отсутствия жесткой типизации данных в потоке.

4.4. Содержание самостоятельной работы

Разделы, темы, дидактические единицы
Тема 1. Основы теории криптографических протоколов: классификация, свойства и формальные модели Вводятся формальные методы описания и верификации с использованием BAN-логики (<i>Logic of Beliefs</i>), позволяющей математически доказать отсутствие логических ошибок в последовательности обмена сообщениями.
Тема 2. Протоколы идентификации и строгой аутентификации сторон Практическая часть посвящена разбору механизмов <i>CHAP</i> (<i>Challenge Handshake Authentication Protocol</i>) и протоколов на основе симметричного шифрования (<i>Needham-Schroeder Shared-Key Protocol</i>), а также их модификаций для устранения известных недостатков.
Тема 3. Протоколы распределения ключей: Диффи-Хеллмана и Керберос Анализируется архитектура сети доверия <i>Kerberos</i> как централизованной системы выдачи сеансовых билетов (<i>TGS/AS</i>). Описывается процесс получения билета на получение билетов (<i>TGT</i>) и последующего доступа к сервису, включая защиту от перехвата паролей и повторного использования билетов.
Тема 4. Построение защищенных каналов связи: TLS 1.3 и IPsec Для сетевого уровня (<i>IPsec</i>) рассматриваются архитектуры <i>AH</i> (<i>Authentication Header</i>) и <i>ESP</i> (<i>Encapsulating Security Payload</i>), режимы работы (<i>транспортный</i> и <i>туннельный</i>), а также протокол автоматического управления ключами <i>IKEv2</i> .
Тема 5. Схемы электронной подписи и протоколы неоспоримости (Non-repudiation) Концепция службы доверенного времени (<i>Timestamping Authority - TSA</i>) и квитанций о доставке (<i>Delivery Receipt</i>), которые необходимы для реализации свойства неотрекаемости в системах электронного документооборота согласно стандартам типа <i>CAdES/XAdES</i> .
Тема 6. Атаки на криптографические протоколы и методы их анализа Атаки на побочные каналы (<i>Side-channel attacks</i>): извлечение ключей через измерение времени выполнения операций или потребления энергии. Для противодействия изучаются инструменты формальной проверки моделей (<i>ProVerif</i> , <i>Scyther</i>), позволяющие автоматически найти сценарии атак на описанную спецификацию протокола.

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 с оценкой. 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. Кочуров, Л. А. Криптографические алгоритмы, модели и методы обеспечения информационной безопасности : учебное пособие / Л. А. Кочуров, 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.