БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Ректор Белорусского
государственного университета
_____А.Д.Король
27 июня 2025 г.
Регистрационный № УД-14134/уч.

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Учебная программа учреждения образования по учебной дисциплине для специальности:

1-98 01 01 Компьютерная безопасность (по направлениям)

Направления специальности:

1-98 01 01-01 Компьютерная безопасность (математические методы и программные системы)

2025 г.

Учебная программа составлена на основе ОСВО 1-98 01 01-2021 и учебного плана № Р98-1-206/уч. от 22.03.2022.

СОСТАВИТЕЛЬ:

И.Б.Бережной, доцент кафедры математического моделирования и анализа данных факультета прикладной математики и информатики Белорусского государственного университета, кандидат физико-математических наук

РЕЦЕНЗЕНТ:

А.Л.Костевич, начальник группы разработки средств криптографической защиты информации, ЗАО «Авест», кандидат физико-математических наук

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математического моделирования и анализа данных БГУ
(протокол № 12 от 26.05.2025)

Научно-методическим советом БГУ
(протокол № 11 от 26.06.2025)

Заведующий кафедрой _____ В.И.Малюгин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи дисциплины

Цель дисциплины «Криптографические протоколы»: ознакомление студентов с основами современной теории криптографических протоколов, практическими задачами, решаемыми с помощью криптографических протоколов, а также изучение теоретических и практических аспектов создания, применения и анализа стойкости компьютерных систем с использованием криптографических протоколов.

Задачи учебной дисциплины:

– изучение основных принципов и овладение методологией проектирования криптографических протоколов;

– приобретение навыка практической реализации криптографических протоколов на языке программирования высокого уровня с использованием современных инструментальных средств;

– формирование навыков анализа стойкости криптографических протоколов для обеспечения безопасности в современных информационных системах и компьютерных сетях.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина «Криптографические протоколы» относится к дисциплинам специализации компонента учреждения высшего образования.

Взаимосвязь с другими дисциплинами

Учебная программа составлена с учетом межпредметных связей с учебными дисциплинами. Дисциплина «Криптографические протоколы» основывается на знаниях, полученных при изучении дисциплин «Операционные системы», «Компьютерные сети», «Криптографические методы» и тесно связана с другими дисциплинами специализации.

Требования к компетенциям

Освоение учебной дисциплины «Криптографические протоколы» должно обеспечить формирование следующих компетенций:

Универсальные компетенции:

Решать стандартные задачи профессиональной деятельности на основе применения информационно-коммуникационных технологий.

Специальные компетенции:

Разрабатывать и анализировать надежность блочных и поточных криптосистем, функций хеширования, криптосистем с открытым ключом и систем электронной цифровой подписи.

В результате изучения дисциплины обучаемый должен:

знать:

– типы ключей и их взаимосвязь, функции управления ключами, классификацию способов распределения ключевой информации;

– основные схемы двухсторонних и трехсторонних криптографических протоколов аутентификации, распределения ключей и голосования;

– разновидности атак на криптографические протоколы аутентификации и распределения ключей;

– основные схемы и особенности функционирования реализаций распространенных криптографических протоколов, их уязвимые места и известные атаки;

уметь:

– применять изложенный материал на практике при проектировании криптографических протоколов;

– разрабатывать функции хэширования, системы электронной подписи и криптографические протоколы взаимодействия на языке программирования высокого уровня с использованием современных инструментальных средств;

– анализировать надежность криптосистем, функций хэширования, схем электронной цифровой подписи и криптографических протоколов в целом;

владеть:

– методологией проектирования криптографических протоколов;

– навыками работы с утилитами для анализа безопасности протоколов;

– навыками анализа сетевого трафика в целом и обработки трафика криптографических протоколов.

Структура учебной дисциплины

Дисциплина изучается в 7 семестре. В соответствии с учебным планом всего на изучение учебной дисциплины «Криптографические протоколы» отведено 200 часов, в том числе 72 аудиторных часа, из них: лекции – 36 часов, лабораторные занятия – 36 часов. Из них:

Лекции – 36 часов, лабораторные занятия – 30 часов, управляемая самостоятельная работа – 6 часов.

Трудоёмкость учебной дисциплины составляет 6 зачётных единиц.

Форма промежуточной аттестации – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. Основы криптографических протоколов

Тема 1.1. Основные понятия. Модель угроз Долева-Яо

Предмет и цель курса. Основные определения. Виды протоколов. Задачи, решаемые криптографическими протоколами. Модель угрозы Долева-Яо.

Тема 1.2. Основы работы с сетевым трафиком

Анализ сетевого трафика. ПО Wireshark и его консольная версия. Парсеры протоколов. Генерация сетевого трафика. Реализация сетевого взаимодействия на языке Python. Применение инструмента Scapy для языка Python.

Тема 1.3. Криптографические хэш-функции

Однонаправленные функции. Понятие криптографической хэш-функции и ее свойства. Способы построения хэш-функций. HMAC. Хэш-функции MD5, SHA1 и SHA-2, их сравнительный анализ. Обзор современных стандартов хэш-функций (SHA-3 «Keccak», belt-hash (СТБ 34.101.77-2020), «Стрибог» (ГОСТ Р 34.11-2018), Argon2). Библиотеки хэш-функций для языка Python и их практическое применение. Атаки на хэш-функции. ПО hashcat и его возможности.

Тема 1.4. Электронная цифровая подпись

Электронная цифровая подпись. Определение, решаемые задачи, основные принципы. Классические схемы ЭЦП: RSA, Эль-Гамаля, Шнорра. Схемы ЭЦП на эллиптических кривых: Эль-Гамаля и Нюберг-Рюппеля. Схема слепой подписи Чома. Схема групповой подписи Шнорра. Обзор современных стандартов (DSS FIPS 186-5, ГОСТ Р 34.10-2018, СТБ 34.101.45-2013). Библиотеки ЭЦП для языка Python и их практическое применение.

Тема 1.5. Управление ключами. PKI

Управление ключами. Типы ключей в зависимости от практического использования. Жизненный цикл ключа. Инфраструктура открытых ключей. Структура сертификата X.509. Протокол OCSP. Библиотеки для языка Python для работы с сертификатами и их практическое применение.

Раздел 2. Протоколы аутентификации и распределения ключей

Тема 2.1. Протоколы аутентификации

Определение аутентификации. Виды протоколов аутентификации. Аутентификация на основе паролей. Протоколы аутентификации на базе техники «запрос-ответ». Протоколы ISO с использованием ЭЦП. Схемы аутентификации Фиата-Шамира, Шнорра, Окамото, GQ.

Тема 2.2. Протоколы распределения ключей

Понятия ключевой системы и распределения ключей. Схема предварительного распределения ключей. Протоколы распределения ключей без использования третьей доверенной стороны, основанные на симметричной

криптосистеме. Протокол, использующий необратимые функции. Трехпроходной протокол Шамира. Протоколы распределения ключей с участием третьей доверенной стороны, основанные на симметричной криптосистеме: протоколы стандартов ISO/EEC 9798-2, ISO/IEC 11770-2, протоколы Нидхема-Шредера, Деннинга-Сакко, Ньюмена-Стабблебайна. Протоколы распределения ключей, основанные на асимметричной криптосистеме: протокол Диффи-Хеллмана и его усиления, протокол MTI, протокол Нидхема-Шредера, протокол STS. Протоколы распределения ключей на эллиптических кривых: Диффи-Хэллмана, MQV-протокол, эллиптический вариант Эль-Гамаля. Стандарт СТБ 34.101.66-2014.

Тема 2.3. Формальная верификация протоколов

Понятие формальной верификации криптографического протокола. Свойства информационной безопасности. Обзор методов и ПО для формальной верификации (AVISPA, ProVerif, Scyther).

Раздел 3. Прикладные криптографические протоколы

Тема 3.1. Протокол SSL/TLS

Описание, сфера применения, история версий. Структура и функционирование протокола. Формализованное описание. Состав набора Ciphersuite. Библиотеки, реализующие протокол SSL/TLS, для языка Python и их практическое применение. Обзор атак на протокол SSL/TLS и его реализации. Атака HeartBleed. MITM-атака, практическое использование утилиты sslsplit.

Тема 3.2. Протокол SSH

Стандарты и реализации, сфера использования. Структура SSH. Применение утилит openssh и putty. Особенности настройки клиентской и серверной частей. Атаки на протокол аутентификации. Downgrade-атаки и MITM-атаки.

Тема 3.3. Протокол IPSec VPN

Сфера применения. Общая архитектура протокола. Фазы и режимы IKE. Ограничения, недостатки и уязвимые места протокола. Практическое развертывание IPSec VPN.

Тема 3.4. Протокол Kerberos.

История версий, сфера использования. Логические компоненты и основные принципы работы. Ограничения, недостатки и уязвимые места протокола. Организация доступа к ресурсам с помощью Kerberos. Атаки на Kerberos: перехват аутентификационных данных, Kerberoasting, Silver/Golden Ticket, Pass-the-Ticket. Применение утилит Rubeus и mimicatz.

Тема 3.5. Протокол NTLM

Описание протокола, история версий, сфера использования. Хэши NTLM, схема генерации, механизм вскрытия с помощью hashcat. Атака Pass-the-Hash.

Раздел 4. Протоколы в недоверенной среде

Тема 4.1. Схемы разделения секрета. Протоколы голосования

Схемы разделения секрета Шамира и Блэкли, пороговые схемы. Стандарт СТБ 34.101.60-2014. Понятие протокола голосования. Протокол голосования с использованием слепой подписи. Протокол голосования с доверенным посредником. Протокол децентрализованного голосования.

Тема 4.2. Блокчейн-протоколы

Блокчейн. Принципы функционирования. Используемые криптографические протоколы. Иерархические кошельки. Протоколы Proof-of-Work, Proof-of-Stake. Технология Lightning. Взаимодействие с блокчейнами на языке Python.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Очная (дневная) форма получения высшего образования с применением дистанционных образовательных технологий (ДОТ)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов				Количество часов УСР	Форма контроля
		Лекции	Практические занятия	Лабораторные занятия	Иное		
1	**Основы криптографических протоколов.**	**14**		**14**			
1.1	Основные понятия. Модель угроз Долева-Яо.	4					Экспресс-опрос
1.2	Основы работы с сетевым трафиком.			4			Отчет по лабораторной работе, контрольная работа
1.3	Криптографические хэш-функции	4		4			Отчет по лабораторной работе, контрольная работа
1.4	Электронная цифровая подпись	4		4			Отчет по лабораторной работе, контрольная работа
1.5	Управление ключами. PKI	2		2			Отчет по лабораторной работе, экспресс-опрос
2	**Протоколы аутентификации и распределения ключей**	**8**		**6**		**2**	
2.1	Протоколы аутентификации	2		2			Отчет по лабораторной работе, контрольная работа
2.2	Протоколы распределения ключей	4		2		2	Отчет по лабораторной работе, контрольная работа

2.3	Формальная верификация протоколов	2		2			Отчет по лабораторной работе
3	**Прикладные криптографические протоколы.**	**10**		**10**			
3.1	Протокол SSL/TLS	2		2			Отчет по лабораторной работе, экспресс-опрос
3.2	Протокол SSH	2		2			Отчет по лабораторной работе, контрольная работа
3.3	Протокол IPSec	2		2			Отчет по лабораторной работе, экспресс-опрос
3.4	Протокол Kerberos	2		2			Отчет по лабораторной работе, экспресс-опрос
3.5	Протокол NTLM	2		2			Отчет по лабораторной работе, контрольная работа
4	**Протоколы в недоверенной среде**	**4**				**4**	
4.1	Схемы разделения секрета. Протоколы голосования	2				2	Экспресс-опрос, контрольная работа
4.2	Блокчейн-протоколы	2				2	Экспресс-опрос
Всего		**36**		**30**		**6**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Криптология: учебник для студентов учреждений высшего образования по математическим и техническим специальностям / [Ю. С. Харин и др.]; БГУ. – 2-е изд., пересмотр. – Минск: БГУ, 2023. – 511 с. – URL: **https://elib.bsu.by/handle/ 123456789/309839**.
2. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание, доп. и испр. / В. Олифер, Н. Олифер – 6-е изд. – Спб.: Питер, 2024. – 1008 с. – (Серия “Учебник для вузов”) – ISBN 978-5-4461-4085-5.
3. Вонг Д. Реальная криптография / пер. с англ. Д. Романовская. – СПб.: Питер, 2024. — 432 с.: ил. – (Серия «Библиотека программиста»). – ISBN 978-5-4461-2091-8
4. Омассон Ж.-Ф. О криптографии всерьез / пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2021. – 328 с. – ISBN 978-5-97060-975-0
5. Boyd C. Protocols for Authentication and Key Establishment. Second Ed. / C. Boyd, A. Mathuria, D. Stebila – Springer Berlin, Heidelberg, 2020. – 521 p. – ISBN 978-3-662-58146-9.

Дополнительная литература

1. Криптографические протоколы. Основные свойства и уязвимости : учеб. пособие для студ. учрежд. высш. проф. образования /А. В. Черемушкин. – М.: Издательский центр «Академия», 2009. — 272 с.
2. Прохорова, О. В. Информационная безопасность и защита информации: учебник / О. В. Прохорова. - 3-е изд., стереотип. - СПб.; М.; Краснодар: Лань, 2021. - 124 с. - ISBN 978-5-8114-7970-2.
3. Нестеренко, А. Ю. Методика оценки безопасности криптографических протоколов. / А. Ю. Нестеренко, А. М. Семенов // Прикладная дискретная математика, 2022 – № 56. – с. 33-82.
4. Шнайер, Б. Прикладная криптография: протоколы, алгоритмы и исходные коды на языке С / Б. Шнайер; [пер. с англ. и ред. Д. А. Клюшина]. – 2-е (юбил.) изд. – СПб: ООО «Диалектика», 2022. – 1040 с.

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

На лекционных занятиях по дисциплине «Криптографические протоколы» рекомендуется особое внимание обращать внимание на установление связей между теоретическим темами дисциплины и использованием изучаемых методов для решения практических задач.

Контрольные мероприятия проводятся в соответствии с учебно-методической картой дисциплины.

Для диагностики компетенций в рамках учебной дисциплины рекомендуется использовать следующие формы:

- Устная форма: экспресс-опрос.
- Письменная форма: контрольные работы.
- Устно-письменная форма: отчеты по лабораторным работам с их устной защитой.

Формой промежуточной аттестации по дисциплине учебным планом предусмотрен экзамен.

Для формирования итоговой отметки по учебной дисциплине используется модульно-рейтинговая система оценки знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая система предусматривает использование весовых коэффициентов для текущей и промежуточной аттестации студентов по учебной дисциплине.

Формирование итоговой отметки в ходе проведения контрольных мероприятий текущей аттестации (примерные весовые коэффициенты, определяющие вклад текущей аттестации в отметку при прохождении промежуточной аттестации):

- контрольные работы – 50 %;
- отметки за отчёты по лабораторным работам – 30 %;
- устный опрос – 20 %.

Итоговая отметка по дисциплине рассчитывается на основе итоговой отметки текущей аттестации (модульно-рейтинговой системы оценки знаний) 60 % и экзаменационной отметки 40 %.

Примерный перечень заданий для управляемой самостоятельной работы студентов

Управляемая самостоятельная работа (УСР) студентов – это самостоятельная работа, выполняемая по заданию и при методическом руководстве преподавателя, а также контролируемая преподавателем на определенном этапе обучения. Целью УСР является целенаправленное обучение студентов основным навыкам и умению индивидуальной самостоятельной работы.

На освоение учебного материала в рамках УСР для дисциплины «Криптографические протоколы» отводится 6 аудиторных часов по трем следующим темам в соответствии с учебно-методической картой дисциплины.

Тема 2.2. Протоколы распределения ключей (2 часа)

Перечень вопросов для углубленного самостоятельного изучения:

- эллиптический вариант протокола Диффи-Хэллмана;
- протокол MQV (Менезеса-Кью-Ванстоуна).

- протокол MTI.

Форма контроля – отчет по лабораторной работе.

Тема 4.1. Схемы разделения секрета. Протоколы голосования (2 часа)

Перечень вопросов для углубленного самостоятельного изучения:

- Схема разделения секрета Шамира.
- Схема разделения секрета Блэкли.

Форма контроля – контрольная работа

Тема 4.2. Блокчейн-протоколы. (2 часа)

Перечень вопросов для углубленного самостоятельного изучения:

- Иерархические кошельки.
- Взаимодействие с блокчейном Bitcoin на языке Python.

Форма контроля – экспресс-опрос.

Примерный план проведения отдельных лабораторных занятий

1. Основы работы с сетевым трафиком. Инструментарий Scapy.

Цель: умение генерировать сетевой трафик заданного вида

Задачи по теме занятия:

1). С помощью Python-библиотеки Scapy сформировать ICMP-пакет с заданной нагрузкой, отобразить его структуру и послать его в сеть.

2) Сформировать HTTP-пакет с заданной нагрузкой-запросом, послать его в сеть и проанализировать полученный ответ.

3) Используя возможности Python-библиотеки Scapy организовать сканирование заданного диапазона портов на узле с заданным IP-адресом.

4) Реализовать мониторинг заданного количества проходящих сетевых пакетов.

2. Хэш-функции. ПО hashcat и его возможности.

Цель: умение восстановить прообраз для заданного хэш-значения путем перебора кандидатов

Задачи по теме занятия:

1) Вычислить для заданного слова MD5-хэш. Проверить возможность восстановления прообраза по стандартному словарю. Изучить статистику процесса для различных режимов запуска.

2) Провести попытку восстановления прообраза заданного MD5-хэша путем полного перебора по заданной маске.

3) Провести попытку восстановления прообраза заданного MD5-хэша путем перебора по словарю с учетом определенных мутаций для слов-кандидатов.

4) Рассмотреть варианты повышения скорости перебора путем дополнительной настройки опций запуска ПО hashcat.

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используется практико-ориентированный подход, который предполагает:

- освоение содержание образования через решения практических задач;
- приобретение навыков эффективного выполнения разных видов профессиональной деятельности;
- ориентацию на генерирование идей, реализацию групповых студенческих проектов;
- использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

Методические рекомендации по организации самостоятельной работы обучающихся

Студенты самостоятельно выполняют следующую работу:

- осуществляют углубленное изучение тем с использованием рекомендуемой литературы;
- выполняют лабораторные задания с использованием различных программных инструментов;
- работают над устранением недостатков, указанных при приемке отчётов.

Для организации самостоятельной работы студентов по учебной дисциплине следует разместить на образовательном портале комплекс учебных и учебно-методических материалов (учебно-программные материалы, методические указания к лабораторным занятиям, материалы текущего контроля и текущей аттестации, список рекомендуемой литературы, информационных ресурсов и др.).

Примерный перечень вопросов к экзамену

1. Криптографические протоколы. Основные определения и задачи.
2. Модель угроз Долева-Яо. Разновидности атак на протоколы.
3. Однонаправленные функции. Понятие криптографической хэш-функции. Свойства хэш-функции.
4. Хэш-функции MD4, MD5 и SHA1, их сравнительный анализ.
5. Обзор современных стандартов хэш-функций (SHA-3 «Keccak», Argon2, belt-hash (СТБ 34.101.31-2011), «Стрибог» (ГОСТ Р 34.11-2012)).
6. ПО hashcat, его возможности и особенности работы.
7. Электронная цифровая подпись. Определение, решаемые задачи, основные принципы. Структурная классификация.
8. Классические схемы ЭЦП: RSA, Фиата-Шамира, Эль-Гамаля, Шнорра.
9. Схемы ЭЦП на эллиптических кривых: Эль-Гамаля и Нюберг-Рюппеля.

10. Схема слепой подписи Чома. Схема групповой подписи Шнорра.

11. Современные стандарты ЭЦП (DSS, ГОСТ Р 34.10-2012, СТБ 34.101.45-2013).

12. Управление ключами. Типы ключей в зависимости от практического использования. Жизненный цикл ключа. Инфраструктура открытых ключей.

13. Определение аутентификации. Виды протоколов аутентификации. Аутентификация на основе паролей. Протоколы аутентификации на базе техники «запрос-ответ».

14. Схемы аутентификации Фиата-Шамира, Шнорра.

15. Понятие ключевой системы. Распределение ключей. Классификация способов распределения ключей. Предварительное распределение ключей.

16. Протоколы распределения ключей без использования третьей доверенной стороны, основанные на симметричной криптосистеме. Протокол, использующий необратимые функции, протокол с использованием MAC-кода.

17. Протоколы Нидхема-Шредера, Деннинга-Сакко, Ньюмена-Стабблебайна.

18. Протокол Диффи-Хеллмана и его усиления.

19. Протокол STS, протокол MTI.

20. Протоколы распределения ключей на эллиптических кривых: Диффи-Хэллмана, MQV-протокол, эллиптический вариант Эль-Гамаля.

21. Стандарт СТБ 34.101.66-2014.

22. Понятие формальной верификации криптографического протокола. Свойства информационной безопасности. Методы формальной верификации.

23. Протокол SSL/TLS. Структура и функционирование протокола. Формализованное описание. Downgrade-атаки.

24. Протокол SSL/TLS. Состав набора Ciphersuite. Схема MITM-атаки.

25. Протокол SSH. Стандарты и реализации, сфера использования. Структура SSH.

26. Протокол IPSec VPN. Сфера применения. Архитектура протокола. Формальное описание компонент.

27. Протокол Kerberos. Логические компоненты и основные принципы работы, формальное описание протокола. Ограничения, недостатки и уязвимые места протокола.

28. Основные схемы атак на протокол Kerberos: перехват аутентификационных данных, Kerberoasting, Silver/Golden Ticket, Pass-the-Ticket.

29. Протокол NTLM. История версий, сфера использования. Хэши NTLM, схема генерации, механизм вскрытия с помощью ПО hashcat.

30. Протокол NTLM. Механизм атаки Pass-the-Hash.

31. Схемы разделения секрета Шамира и Блэкли.

32. Понятие протокола голосования. Протокол голосования с использованием слепой подписи.

33. Блокчейн. Принципы функционирования. Используемые криптографические примитивы.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Учебная дисциплина не требует согласования			

Заведующий кафедрой математического моделирования и анализа данных
доктор эконом. наук, профессор В.И.Малюгин

26.05.2025

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УО

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 202_ г.)
Заведующий кафедрой
_____ _____

УТВЕРЖДАЮ
Декан факультета
_____ _____