ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

**УТВЕРЖДЕНА**

Решением Ученого совета
АНО ВО «Центральный университет»
«07» марта 2024 г.
Протокол № 1

**Рабочая программа дисциплины (модуля)**
**«Прикладная криптография»**

**Направление подготовки:** *02.03.01 Математика и компьютерные науки*

**Направленность (профиль) подготовки:** *Разработка*

**Квалификация (степень) выпускника:** *бакалавр*

**Форма обучения:** *очная*

**Срок освоения программы:** *4 года*

**Год набора:** *2024*

**Москва**
**2024**

Электронный документ

**Содержание**

1. **Краткая характеристика дисциплины (модуля)** ..... 3
2. **Перечень планируемых результатов обучения** ..... 5
3. **Тематический план** ..... 7
4. **Содержание дисциплины (модуля)** ..... 7
5. **Учебно-методическое обеспечение** ..... 8
6. **Материально-техническое обеспечение** ..... 8
7. **Методические и оценочные материалы** ..... 10

## 1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Прикладная криптография» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению 02.03.01 «Математика и компьютерные науки», профиль «Разработка», утвержденный приказом Министерства науки и высшего образования Российской Федерации № 807 от 23.08.2017 года.

Изучение дисциплины (модуля) «Прикладная криптография» позволяет обеспечить подготовку специалистов в области информационной безопасности, обеспечения защиты данных в цифровой экономике, государственных и коммерческих системах, а также для противодействия киберугрозам.

**Место дисциплины (модуля) в структуре образовательной программы**

Настоящая дисциплина (модуль) включена в учебный план по программе подготовки бакалавриата по направлению 02.03.01 «Математика и компьютерные науки», профиль «Разработка» и входит в вариативную часть Блока 1, формируемую участниками образовательных отношений, как дисциплина по выбору.

Дисциплина (модуль) изучается на 3,4 курсе в 5 или 6,7 семестре по выбору после успешного освоения одной из дисциплин (модулей): «Архитектура компьютера и операционные системы. Часть 1», «Разработка на C++», «Алгоритмы и структуры данных. Часть 1» или «Алгоритмы и структуры данных. Часть 1. Продвинутый уровень».

**Цель изучения дисциплины (модуля):** формирование у студентов систематизированных знаний и практических навыков в области современной криптографии, направленных на обеспечение конфиденциальности, целостности, аутентичности и неотказуемости информации в информационных системах и сетях.

**Задачи изучения дисциплины (модуля)**:

— изучить основы и принципы криптографии;

— освоить симметричные и асимметричные алгоритмы, хэш-функции;

— научиться применять криптографию на практике (шифрование, цифровая подпись, управление ключами);

— познакомиться с криптопротоколами (TLS, SSH, IKE) и стандартами (ГОСТ, AES, RSA);

— оценивать безопасность криптосистем и уязвимости к атакам.

**В результате освоения дисциплины (модуля) обучающийся должен:**

***знать:***

— основные понятия криптографии: криптографический примитив, схема, протокол, защищённая система;

— методы симметричного шифрования, асимметричной криптографии, хеш-функций, mac, aead, цифровых подписей и сертификатов;

— базовую логику работы tls;

— основные свойства криптографических хеш-функций и причины, по которым устаревшие хеши не применяются в задачах криптографической защиты;

— назначение блочных шифров, режимов их работы;

— основные идеи rsa и ecc как механизмов асимметричной криптографии;

— понятие атаки man-in-the-middle и роль инфраструктуры доверия в её предотвращении;

— типовые ошибки применения криптографии;

— общую идею постквантовой миграции и необходимость проектирования систем, допускающих замену криптографических механизмов;

***уметь:***

— анализировать криптографическую систему, выделяя в ней примитивы, схемы,

протоколы, ключи и доверительные границы;

— применять симметричное шифрование с корректным указанием алгоритма, режима, ключа и iv/nonce;

— вычислять и сравнивать криптографические хеши файлов и сообщений;

— проверять целостность и подлинность сообщения с использованием mac, hmac или aead;

— выполнять базовые операции с rsa: расшифрование, проверку подписи, интерпретацию padding и параметров подписи;

— проверять цифровые подписи и различать задачи шифрования, подписи и аутентификации;

— анализировать сертификаты и цепочки доверия, выявлять ошибки проверки сертификата;

— разбирать упрощённый tls-сценарий и определять, где устанавливается доверие и защищённый канал;

— выявлять типовые ошибки в криптографической схеме или конфигурации;

— составлять формализованный результат анализа в заданном формате;

***владеть:***

— навыками практического анализа криптографических решений от алгоритма до защищённой системы;

— навыками работы с криптографическими параметрами;

— методикой проверки корректности криптографической операции: расшифрования, проверки подписи, проверки целостности и проверки сертификата;

— навыками диагностики распространённых ошибок применения криптографии;

— практикой анализа защищённого канала на уровне установления доверия, обмена ключами и защиты передаваемых данных;

— методикой выбора подходящего криптографического механизма под задачу: шифрование, хеширование, mac, подпись, aead;

— навыками формализованного аудита небольшой криптографической архитектуры;

— навыками оценки системы с точки зрения устойчивости к mitm и корректности инфраструктуры доверия;

— подходами к оценке готовности системы к смене криптографических алгоритмов;

— опытом краткой технической защиты полученного решения.

## 2. Перечень планируемых результатов обучения

Компетенции, формируемые в результате освоения дисциплины (модуля) при проведении учебных занятий в форме контактной работы обучающихся с педагогическими работниками Университета и в форме самостоятельной работы обучающихся:

| Компетенция | Содержание компетенции | Индикатор компетенции | Перечень планируемых результатов обучения по дисциплине (модулю) |
|---|---|---|---|
| УК-1. | Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | УК-1.1. | Знает методы поиска и анализа информации в области разработки, основные принципы критической оценки источников информации и их релевантности |
| | | УК-1.2. | Умеет критически оценивать источники информации и синтезировать данные из различных источников для решения задач, применять системный подход к анализу и решению комплексных проблем |
| | | УК-1.3. | Имеет практический опыт работы с современными инструментами и технологиями для обработки информации, формулировании и структурировании задач на основе полученной информации |
| УК-2. | Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | УК-2.1. | Знает действующие правовые нормы, регулирующие деятельность в области решения задач, основные методы и подходы к определению круга задач |
| | | УК-2.2. | Умеет определять круг задач в рамках поставленной цели, выбирать оптимальные способы решения задач, учитывая имеющиеся ресурсы и ограничения |
| | | УК-2.3. | Имеет практический опыт применения знаний о правовых нормах и ресурсах в реальных ситуациях, разработки и реализации решений в соответствии с установленными ограничениями |
| ОПК-1. | Способен консультировать и использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа алгебры, | ОПК-1.1. | Знает основные концепции и теории в области математического анализа и смежных дисциплин; методы и подходы, используемые в различных областях математики |
| | | ОПК-1.2. | Умеет применять математические методы для решения профессиональных задач |

| | | | |
|---|---|---|---|
| | аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в профессиональной деятельности | ОПК-1.3. | Имеет практический опыт разработки и реализация математических моделей в профессиональной деятельности |
| ПК-1. | Способен формулировать задачи с математической точностью, обосновывать утверждения строго и анализировать полученные результаты в области математики и компьютерных наук | ПК-1.1. | Обладает базовыми знаниями, полученными в области математических наук, программирования и информационных технологий |
| | | ПК-1.2. | Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в математике и информатике |
| | | ПК-1.3. | Имеет опыт работы с задачами в области математики и компьютерных наук, включая применение математических методов для решения практических задач |
| ПК-2. | Способен решать типовые задачи профессиональной деятельности в области разработки, опираясь на информационную и библиографическую культуру, используя информационно-коммуникационные технологии и учитывая основные требования информационной безопасности | ПК-2.1. | Знает основные принципы информационной и библиографической культуры, а также правила и стандарты информационной безопасности |
| | | ПК-2.2. | Умеет эффективно использовать информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности с учетом требований информационной безопасности |
| | | ПК-2.3. | Имеет практический опыт работы с информационными ресурсами и инструментами в рамках своей профессиональной деятельности в области разработки, соблюдая требования информационной безопасности |

## 3. Тематический план

| №п/п | Наименование раздела дисциплины (модуля) | Трудоемкость, академические часы | | | | ТКУ (текущий контроль успеваемости) |
|---|---|---|---|---|---|---|
| | | *Очная форма* | | | | |
| | | Аудиторная работа | | Контроль | Самостоятельная работа | |
| | | Лекции | Семинары (практические занятия) | | | |
| 1 | Современный защищённый канал и модель угроз | 4 | 4 | | 20 | Домашнее задание 1 |
| 2 | Идентичность, подписи и классическая асимметрия | 4 | 4 | 4 | 20 | Домашнее задание 2 |
| 3 | Защита данных: хеши, шифрование, целостность | 8 | 8 | 4 | 20 | Домашнее задание 2 |
| 4 | Доверие в протоколах: PKI, TLS 1.3, ECC | 6 | 6 | | 30 | Домашнее задание 1 |
| 5 | Криптография в инфраструктуре и национальных профилях | 2 | 2 | 4 | 36 | Домашнее задание 1 |
| | ***Зачет с оценкой*** | | | 4 | | Проект |
| | ***Итого:*** | ***24*** | ***24*** | ***16*** | ***126*** | |
| ***Объем дисциплины (модуля) (в ак. ч.)*** | | ***190*** | | | | |
| ***Объем дисциплины (модуля) (в зач. ед.)*** | | ***5*** | | | | |

## 4. Содержание дисциплины (модуля)

| №п/п | Наименование раздела дисциплины (модуля) | Содержание дисциплины (модуля) по темам |
|---|---|---|
| 1 | Современный защищённый канал и модель угроз | TLS как повседневная криптография<br>Открытые ключи, распределение ключей и MITM |
| 2 | Идентичность, подписи и классическая асимметрия | RSA: идея, функция Эйлера, модуль, генерация ключей<br>RSA в реальных системах: дополнение, подписи, размеры ключей<br>Контроль теоретических знаний 1 |
| 3 | Защита данных: хеши, шифрование, целостность | Хеши и пароли: MD5, SHA, Стрибог. Утилита hashcat<br>Шифрование данных: AES и Кузнечик<br>Режимы работы шифров: CBC, CTR, IV, nonce<br>Целостность и AEAD: MAC, HMAC, GCM, MGM<br>Контроль теоретических знаний 2 |
| 4 | Доверие в протоколах: PKI, TLS 1.3, ECC | Сертификаты, X.509 и цепочка доверия<br>TLS подробно: рукопожатие, протокол записей, прямая секретность<br>ECC и современная асимметрия |
| 5 | Криптография в инфраструктуре и национальных профилях | Российские криптографические профили и инфраструктурная интеграция<br>Проект |

## 5. Учебно-методическое обеспечение

Университет располагает полным набором лицензионного и свободно распространяемого программного обеспечения, включая продукты отечественного производства.

Каждый студент в течение всего периода обучения получает индивидуальный неограниченный доступ к электронно-библиотечной системе и электронной информационно-образовательной среде университета. Эти системы предоставляют возможность доступа к ресурсам из любой точки, где есть подключение к сети Интернет, как на территории университета, так и за его пределами.

Студентам обеспечен удаленный доступ к современным профессиональным базам данных и информационным справочным системам.

***Основная литература:***

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2026. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583783

2. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536453

3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2026. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583633

***Дополнительная литература:***

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2026. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584129

## 6. Материально-техническое обеспечение

Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Изучение дисциплины (модуля) обеспечивается в учебных аудиториях, оснащенных:

— столами и стульями;

— компьютерной техникой;

— механическими калькуляторами;

— специализированным оборудованием, включая демонстрационное оборудование.

Помещения для самостоятельной работы обучающихся, в том числе приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

Обучающимся предоставляется доступ (в том числе удаленный) к ресурсам информационно-телекоммуникационной сети «Интернет», электронным ресурсам (в том числе электронным библиотечным системам, современным профессиональным базам данных и информационным справочным системам):

| № | Наименование портала (издания, курса, документа) | Ссылка |
|---|---|---|
| 1. | Научная электронная библиотека elibrary.ru библиотека | https://elibrary.ru/defaultx.asp |
| 2. | База данных для IT-специалистов | https://habr.com |
| 3. | База данных ScienceDirect | https://www.sciencedirect.com |
| 4. | Официальный сайт Министерства науки и высшего образования Российской Федерации | https://minobrnauki.gov.ru/ |
| 5. | Федеральный портал «Российское образование" | https://www.edu.ru/ |
| 6. | Информационная система "Единое окно доступа к образовательным ресурсам" | http://window.edu.ru/ |
| 7. | Единая коллекция цифровых образовательных ресурсов | http://school-collection.edu.ru/ |
| 8. | Федеральный центр информационно - образовательных ресурсов | http://fcior.edu.ru/ |

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), в том числе комплект лицензионного программного обеспечения, современные профессиональные базы данных и информационные справочные системы:

| Наименование ПО | Производство | Лицензионное / свободно распространяемое |
|---|---|---|
| **Операционные системы:** | | |
| Microsoft Imagine (Windows Client, Server) | зарубежное | лицензионное |
| **Браузеры:** | | |
| Яндекс.Браузер | отечественное | свободно распространяемое |
| Google Chrome | зарубежное | свободно распространяемое |
| **Офисные приложения:** | | |
| Microsoft Imagine (Visio, OneNote) | зарубежное | лицензионное |
| TeXstudio | зарубежное | свободно распространяемое |
| Adobe Acrobat Reader | зарубежное | свободно распространяемое |
| **Программное обеспечение для планирования и учета времени:** | | |
| Toggle app | зарубежное | свободно распространяемое |
| **Системы управления проектами:** | | |
| Microsoft Imagine (Project) | зарубежное | лицензионное |
| **Системы управления базами данных:** | | |
| Microsoft Imagine (SQL Server) | зарубежное | лицензионное |
| **Системы резервного копирования (backup):** | | |
| Acronis Backup Advanced for HyperV | зарубежное | лицензионное |
| **Справочно-правовые системы:** | | |
| КонсультантПлюс: справочно-правовая система | отечественное | лицензионное |

| | | |
|---|---|---|
| **Средства антивирусной защиты:** | | |
| Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition | отечественное | лицензионное |
| **Среды разработки:** | | |
| Visual Studio Code | зарубежное | свободно распространяемое |
| Bash (Unix shell) | зарубежное | свободно распространяемое |
| Anaconda | зарубежное | свободно распространяемое |
| Robotic Operating System | зарубежное | свободно распространяемое |
| CopelliaSim | зарубежное | свободно распространяемое |
| Google Colaboratory | зарубежное | свободно распространяемое |
| **Пакеты программных средств и библиотек:** | | |
| AutoPsy | зарубежное | свободно распространяемое |
| Interactive Disassembler (IDA) | зарубежное | свободно распространяемое |
| **Системы управления библиографической информацией:** | | |
| Zotero | зарубежное | свободно распространяемое |
| **Сервисы и службы:** | | |
| Bind | зарубежное | свободно распространяемое |
| Docker | зарубежное | свободно распространяемое |

## 7. Методические и оценочные материалы

### Методические указания для обучающихся по освоению дисциплины (модуля)

В процессе изучения дисциплины (модуля) «Прикладная криптография» в рамках текущего контроля успеваемости используются такие виды учебной работы, как лекции, семинары, домашние задания, проект, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков профессиональной лексики, закрепление практических профессиональных компетенций, поощрение инициатив.

*Лекция* – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект лекций: кратко и схематично фиксировать основные идеи, выводы и обобщения лекции; выделять важные мысли, ключевые слова и термины. Необходимо отметить вопросы или материалы, которые вызывают затруднения, и попытаться найти ответы в рекомендованной литературе. Если разобраться в материале не удается, следует сформулировать вопрос и задать его преподавателю на консультации или во время семинарского (практического) занятия.

*Семинар* – это форма учебной деятельности, проводимая в учебном заведении под руководством преподавателя, где студенты активно участвуют в обсуждениях, практических заданиях и других формах взаимодействия.

Для успешной подготовки к семинару рекомендуется заранее ознакомиться с темой занятия и основными материалами, чтобы иметь возможность активно участвовать в обсуждении. Также полезно подготовить вопросы и идеи для обсуждения, что поможет глубже понять материал и продемонстрировать заинтересованность.

*Домашнее задание* – набор задач по темам недели.

При работе над домашними заданиями важно внимательно ознакомиться с требованиями и сроками выполнения. Рекомендуется разбивать задания на этапы, чтобы избежать перегрузки и лучше усвоить материал, использовать различные источники информации, включая учебники и онлайн-ресурсы, для более глубокого понимания темы.

*Проект* – исследовательская работа по дисциплине (модулю) и презентация

результатов.

Для успешной подготовки к проекту рекомендуется: четко определить цели и задачи проекта; составить план работы, разбив проект на этапы с указанием сроков выполнения каждого из них; использовать разнообразные источники информации и инструменты для исследования темы; регулярно проверять прогресс и вносить коррективы в план, если это необходимо.

*Самостоятельная работа* – работа студентов, направленная на углубленное изучение отдельных тем и вопросов учебной дисциплины (модуля).

В процессе самостоятельной работы студенты взаимодействуют с рекомендованными материалами при минимальном участии преподавателя. Задачи студента включают работу с конспектами лекций (обработка текста), повторное изучение учебных материалов, планов и тезисов ответов, изучение дополнительных тем, выполнение учебно-исследовательских заданий и другое.

**Система оценивания результатов обучения по дисциплине (модулю)**

**Критерии получения уровня и оценивания сформированности компетенций по дисциплине (модулю) «Прикладная криптография»**

Оценивание уровня учебных достижений, обучающихся по дисциплине (модулю), осуществляется в виде текущего контроля успеваемости и промежуточной аттестации.

**Промежуточная аттестация** по дисциплине (модулю) осуществляется в форме ***зачета с оценкой***, при этом проводится оценка компетенций, сформированных по дисциплине.

Для оценивания текущего контроля успеваемости и промежуточной аттестации используется десятибалльная шкала оценивания, которая соотносится с традиционной пятибалльной шкалой следующим образом:

| **Десятибалльная оценка** | **Пятибалльная оценка** | **Оценка за зачет** | **Общая характеристика результата обучения по дисциплине (модулю)** |
|---|---|---|---|
| 10 | Отлично | Зачтено | Студент полностью владеет знаниями, изложенными в рабочей программе, и глубоко осмысляет дисциплину. Он самостоятельно и логически последовательно отвечает на все вопросы, акцентируя внимание на наиболее важном. Умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя ключевые моменты и устанавливая причинно-следственные связи. Четко формулирует ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты дисциплины (модуля) с практическими |
| 9 | Отлично | Зачтено | |
| 8 | Отлично | Зачтено | |

| Десятибалльная оценка | Пятибалльная оценка | Оценка за зачет | Общая характеристика результата обучения по дисциплине (модулю) |
|---|---|---|---|
| | | | задачами. |
| 7 | Хорошо | Зачтено | Студент обладает знаниями предмета почти в полном объеме рабочей программы и самостоятельно, логически последовательно и всесторонне отвечает на все вопросы, акцентируя внимание на наиболее значимых моментах. Он умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя его ключевые аспекты и устанавливая причинно-следственные связи. Формулирует свои ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные ситуационные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты предмета с практическими задачами. |
| 6 | Хорошо | Зачтено | |
| 5 | Удовлетворительно | Зачтено | Студент обладает базовыми знаниями по дисциплине (модулю), но испытывает трудности при самостоятельных ответах и использует неточные формулировки. В ходе ответов он допускает ошибки, касающиеся сути вопросов. Студент способен решать только самые простые задачи и владеет лишь минимальным набором методов исследования. |
| 4 | Удовлетворительно | Зачтено | |
| 3 | Не сдан | Не зачтено | Студент не овладел обязательным минимумом знаний по предмету и не может ответить на вопросы, даже если преподаватель задает дополнительные наводящие вопросы. |
| 2 | Не сдан | Не зачтено | |
| 1 | Не сдан | Не зачтено | |

Дисциплина (модуль) «Прикладная криптография» оценивается следующим образом:

| Активность | Вес | Количество | Описание |
|---|---|---|---|
| Домашнее задание 1 | 24% | 4 | Набор задач по темам недели |
| Домашнее задание 2 | 44% | 2 | Набор задач по темам недели |
| Зачет с оценкой | 32% | 1 | Проект - исследовательская работа по дисциплине (модулю) и презентация результатов |

**Формула расчёта итоговой оценки по дисциплине (модулю) «Прикладная криптография»:** «0,24 × среднее за домашние задания 1 + 0,44 × среднее за домашние задания 2 + 0,32 × зачет с оценкой».

**Текущий контроль успеваемости обучающихся по дисциплине (модулю)**

**Примерные домашние задания**

**Задание 1:**

1. Опишите модель угроз по типу *Dolev-Yao* в контексте обмена сообщениями между клиентом и сервером.
2. Приведите 3 примера атак (e.g. replay, MITM, spoofing) и укажите, какие свойства безопасности (конфиденциальность, целостность, аутентичность) нарушаются в каждом случае.
3. Объясните, почему предположение о «ненадёжном канале» является основой проектирования защищённых протоколов.

**Задание 2:**

1. Сгенерируйте пару RSA-ключей (можно с помощью OpenSSL или онлайн-инструмента).
2. Подпишите короткое сообщение (например, "exam2025") с использованием приватного ключа.
3. Предоставьте публичный ключ, подпись и сообщение.
4. Объясните, как получатель может проверить подпись, и почему это гарантирует аутентичность и неотказуемость.

**Примерное описание задания и критерии оценивания к проекту**

**Задание:**

Разработать криптографическую схему для безопасной передачи данных между клиентом и сервером. Обосновать выбор алгоритмов, описать этапы установления соединения, обеспечить защиту от основных угроз (MITM, подделка, replay и др.).

**Что включить в проект:**

— Описание сценария (участники, данные, угрозы).

— Выбор и обоснование алгоритмов:

1. шифрование (AES-GCM, ChaCha20),
2. асимметрия (RSA, ECC),
3. хеши и подписи (SHA-256, ГОСТ, ECDSA),
4. протокол (TLS 1.3 или аналог).

— Схема обмена (по шагам или диаграммой): аутентификация, обмен ключами, шифрование.

— Анализ безопасности: защита от MITM, forward secrecy, проверка сертификатов.

— Оценка возможности замены алгоритмов (готовность к постквантовой криптографии).

— Отчёт (5–7 стр., PDF), при необходимости — приложение с кодом.

**Критерии оценивания:**

— Чёткое описание сценария и модели угроз.

— Корректный и обоснованный выбор криптографических алгоритмов.

— Логичная и безопасная схема установления канала.

— Анализ уязвимостей и меры защиты от них.

— Учёт современных требований (например, поддержка смены алгоритмов).

— Качество оформления и ясность изложения.

**Задания для промежуточной аттестации по дисциплине (модулю)**

| № п/п | Задание | Ответ | Компетенция |
|---|---|---|---|
| 1 | Назовите метод шифрования, использующий единый секретный ключ для защиты конфиденциальности данных. | Симметричное шифрование (например, AES) | УК-1 |
| 2 | Определите механизм, позволяющий стороне доказать свою подлинность посредством приватного ключа. | Цифровая подпись (RSA, ECDSA) | ПК-1 |
| 3 | Что обеспечивает защиту целостности и подлинности передаваемого сообщения? | MAC или HMAC / аутентифицированное шифрование | УК-1 |
| 4 | Укажите протокол, позволяющий выработать общий секретный ключ по незащищённому каналу связи. | Протокол Диффи–Хеллмана (DH, ECDH) | УК-2 |
| 5 | На решении какой математической проблемы базируется стойкость алгоритма RSA? | Проблема факторизации больших целых чисел | УК-2 |
| 6 | Чем обеспечивается криптографическая стойкость эллиптических кривых? | Задача дискретного логарифмирования в группе точек эллиптической кривой | ОПК-1 |
| 7 | Какое свойство булевых функций затрудняет анализ шифра при минимальном изменении входных данных? | Лавинный эффект | ПК-2 |
| 8 | Назовите алгебраическую структуру, применяемую при построении криптосистем с открытым ключом. | Конечные поля и группы | ПК-2 |
| 9 | Для защиты от каких угроз предназначен режим работы блочного шифра AEAD? | Конфиденциальность и целостность (например, AES-GCM) | УК-1 |
| 10 | Что используется для генерации псевдослучайных чисел в криптографических системах? | CSPRNG (криптографически стойкий генератор) | ОПК-1 |
| 11 | Какой протокол установления сессии гарантирует свойство forward secrecy? | TLS 1.3 с ECDHE | ОПК-1 |
| 12 | Опишите процедуру проверки подлинности цифрового сертификата. | Проверка электронной подписи ЦС | УК-1 |
| 13 | Сформулируйте принцип проектирования, предполагающий защиту при компрометации части системы. | Защита по умолчанию / defence in depth | УК-1 |
| 14 | Каким способом осуществляется безопасное хранение криптографических ключей? | Изоляция ключей / key separation | ПК-1 |
| 15 | Что позволяет безопасно обновлять криптографические ключи в системе? | Ротация ключей (key rotation) | УК-1 |
| 16 | Перечислите методы аудита криптографических реализаций. | Статический анализ и формальная верификация | УК-2 |
| 17 | На основе какой математической модели анализируют стойкость хеш-функций к коллизиям? | Теория вероятностей и парадокс дней рождения | УК-2 |
| 18 | Чем оценивают устойчивость шифра к дифференциальному криптоанализу? | Моделирование на основе разностных характеристик | ОПК-1 |
| 19 | В какой модели производится формальное доказательство безопасности криптопротокола? | Моделирование в модели случайного оракула | ПК-2 |

Электронный документ

| | | | |
|---|---|---|---|
| 20 | Каким подходом определяют сложность атаки на криптосистему? | Анализ вычислительной сложности (например, $O(2^n)$) | ПК-2 |