

---

**УТВЕРЖДЕНА**

Решением Ученого совета  
АНО ВО «Центральный университет»  
«25» мая 2026 г.  
Протокол №2

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

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

**Направленность (профиль) подготовки:** Прикладной искусственный интеллект

**Квалификация (степень) выпускника:** бакалавр

**Форма обучения:** очная

**Срок освоения программы:** 4 года

**Год набора:** 2026

**Москва  
2026**

## Содержание

|                                                     |    |
|-----------------------------------------------------|----|
| 1. Краткая характеристика дисциплины (модуля) ..... | 3  |
| 2. Перечень планируемых результатов обучения .....  | 5  |
| 3. Тематический план .....                          | 11 |
| 4. Содержание дисциплины (модуля) .....             | 11 |
| 5. Учебно-методическое обеспечение .....            | 12 |
| 6. Материально-техническое обеспечение .....        | 12 |
| 7. Методические и оценочные материалы .....         | 14 |

## **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 «Прикладной искусственный интеллект», 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 «Прикладной искусственный интеллект» и входит в вариативную часть Блока 1, формируемую участниками образовательных отношений, как дисциплина по выбору.

Дисциплина (модуль) изучается на 3 курсе в 5 семестре.

**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 есс 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:

| Код и содержание компетенции                                                                                                         | Индикатор компетенции и 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-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде<br>(соответствует УНК-02)                  | <p>УК-3.1. (УНК-02.01.) Принимает участие в групповом взаимодействии в ходе профессиональной деятельности (базовый)</p> <p>УНК-02.01.01. У-1. Проявляет понимание своей роли в команде</p> <p>УНК-02.01.01. У-2. Умеет ясно выражать свои мысли в группе</p> <p>УНК-02.01.01. У-3. Способен слушать и учитывать мнения других участников команды.</p> <p>УНК-02.01.01. У-4. Умеет давать конструктивную обратную связь</p> <p>УНК-02.01.01. У-5. Умеет работать в команде, проявлять инициативу и поддерживать коллег</p> <p>УНК-02.01.01. У-6. Обладает навыками разрешения конфликтных ситуаций и поиска компромиссов</p> <p>УНК-02.01.01. З-1. Знает основы командной работы, роли и ответственности каждого участника.</p>                                                                                                          |
|                                                                                                                                      | <p>УК-3.2. (УНК-02.02.) Проявляет лидерство и осуществляет наставничество (базовый)</p> <p>УНК-02.02.01. У-1. Умеет мотивировать и вдохновлять команду для достижения общих целей</p> <p>УНК-02.02.01. У-2. Способен организовывать работу группы, распределять обязанности и контролировать выполнение задач</p> <p>УНК-02.02.01. У-3. Умеет делиться знаниями и опытом, оказывать поддержку и осуществлять наставничество коллегам</p> <p>УНК-02.02.01. У-4. Способен принимать ответственные решения и демонстрировать пример профессионализма</p> <p>УНК-02.02.01. З-1. Знает основы лидерства, мотивации и командообразования</p> <p>УНК-02.02.01. З-2. Знает принципы эффективного наставничества и развития персонала</p> <p>УНК-02.02.01. З-3. Знает методы оценки эффективности работы команды и индивидуальных участников</p> |
| ОПК-6. Способен разрабатывать алгоритмы и компьютерные программы,                                                                    | ОПК-6.1. Знает принципы алгоритмизации, основные структуры данных, парадигмы программирования, методы разработки, тестирования и отладки компьютерных программ.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| пригодные для практического применения                                                         | ОПК-6.2. Умеет разрабатывать, документировать, тестировать и отлаживать алгоритмы и компьютерные программы, пригодные для практического применения, с использованием современных языков и сред разработки.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                                                                                | ОПК-6.3. Имеет практический опыт разработки и сопровождения компьютерных программ и программных комплексов для решения прикладных задач.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| ППК-ДА3. Способен проводить аналитические исследования с применением технологий больших данных | <p>ППК-ДА3.2. – Обеспечивает соответствие результатов анализа бизнес-задачам заказчика (средний)</p> <p>ППК-ДА3.2. 3-1. Знает методы перевода бизнес-требований в аналитические задачи</p> <p>ППК-ДА3.2. 3-2. Знает ключевые бизнес-метрики в предметной области</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ППК-Р5. Способен разрабатывать требования и проектировать программное обеспечение              | <p>ППК-Р5.1. Анализирует возможности реализации требований к компьютерному программному обеспечению (средний)</p> <p>ППК-Р5.1. 3-1. Знает возможности существующей программно-технической архитектуры.</p> <p>ППК-Р5.1. 3-2. Знает возможности современных и перспективных средств разработки программных продуктов, технических средств.</p> <p>ППК-Р5.1. 3-3. Знает методологии разработки компьютерного программного обеспечения и технологии программирования.</p> <p>ППК-Р5.1. У-1. Умеет проводить сбор и систематизацию требований к компьютерному программному обеспечению.</p> <p>ППК-Р5.1. У-2. Умеет выявлять взаимосвязи и документировать требования к компьютерному программному обеспечению</p> <p>ППК-Р5.1. У-3. Умеет вырабатывать варианты реализации требований к компьютерному программному обеспечению.</p> |
|                                                                                                | <p>ППК-Р5.2. Разрабатывает технические спецификации на программные компоненты и их взаимодействие (средний)</p> <p>ППК-Р5.2. 3-1. Знает методы и средства проектирования компьютерного программного обеспечения.</p> <p>ППК-Р5.2. 3-2. Знает методы и средства проектирования программных интерфейсов.</p> <p>ППК-Р5.2. У-1. Умеет выбирать средства реализации требований к компьютерному программному обеспечению.</p> <p>ППК-Р5.2. У-2. Умеет вырабатывать варианты реализации компьютерного программного обеспечения.</p> <p>ППК-Р5.2. У-3. Умеет проводить оценку и обоснование рекомендуемых решений.</p>                                                                                                                                                                                                                  |
|                                                                                                | <p>ППК-Р5.3. Проектирует компьютерное программное обеспечение (продвинутый)</p> <p>ППК-Р5.3. 3-1. Знает принципы построения и виды архитектуры компьютерного программного обеспечения.</p> <p>ППК-Р5.3. 3-2. Знает типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке компьютерного программного обеспечения.</p> <p>ППК-Р5.3. 3-3. Знает нормативно-технические документы (стандарты), определяющие требования к технической документации на компьютерное программное обеспечение.</p> <p>ППК-Р5.3. 3-4. Знает методы и средства проектирования компьютерного программного обеспечения.</p>                                                                                                                                                                                 |

|                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                 | <p>ППК-Р5.3. У-1. Умеет разрабатывать и изменять архитектуру компьютерного программного обеспечения и согласовывать ее с системным аналитиком и архитектором программного обеспечения.</p> <p>ППК-Р5.3. У-2. Умеет проектировать структуры данных.</p> <p>ППК-Р5.3. У-3. Умеет проектировать программные интерфейсы.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                                                                 | <p>ППК-Р5.4. Выполняет логическое проектирование системы (продвинутый)</p> <p>ППК-Р5.4. З-1. Знает устройство и функционирование ИТ-систем/продуктов</p> <p>ППК-Р5.4. З-2. Знает методы моделирования и описания устройства и функционирования ИТ-систем/продуктов, их частей, обеспечения и окружения</p> <p>ППК-Р5.4. З-3. Знает базовые технологии взаимодействия и интеграции систем и компонентов</p> <p>ППК-Р5.4. З-4. Знает методы функциональной декомпозиции ИТ-систем</p> <p>ППК-Р5.4. У-1. Умеет декомпонировать ИТ-системы и ИТ-продукты на подсистемы и элементы поставки</p> <p>ППК-Р5.4. У-2. Умеет описывать интерфейсы пользователя на логическом уровне</p> <p>ППК-Р5.4. У-3. Умеет описывать интеграции со смежными системами на логическом уровне</p> |
| ППК-Р6. Способен участвовать в промышленной разработке программного обеспечения | <p>ППК-Р6.1. Работает в соответствии с промышленными методологиями разработки (средний)</p> <p>ППК-Р6.1. З-1. Знает принципы Agile и их применение в промышленных проектах.</p> <p>ППК-Р6.1. З-2. Знает процессы code review, принципы коллективного владения кодом (collective code ownership).</p> <p>ППК-Р6.1. У-1. Умеет оценивать объем задачи и срок ее выполнения, участвовать в планировании спринтов.</p> <p>ППК-Р6.1. У-2. Умеет работать в команде с использованием инструментов управления проектами.</p>                                                                                                                                                                                                                                                     |
|                                                                                 | <p>ППК-Р6.2. Использует инструменты промышленной разработки (средний)</p> <p>ППК-Р6.2. З-1. Знает принципы Continuous Integration and Continuous Delivery (CI/CD).</p> <p>ППК-Р6.2. З-2. Знает системы мониторинга и логирования в продуктивной среде.</p> <p>ППК-Р6.2. У-1. Умеет настраивать потоки работ CI/CD.</p> <p>ППК-Р6.2. У-2. Умеет работать с контейнеризацией и оркестрацией.</p> <p>ППК-Р6.2. У-3. Умеет настраивать мониторинг в продуктивной среде.</p>                                                                                                                                                                                                                                                                                                   |
|                                                                                 | <p>ППК-Р6.3. Разрабатывает масштабируемый и поддерживаемый код (продвинутый)</p> <p>ППК-Р6.3. З-1. Знает принципы чистого кода, SOLID, DRY, KISS и др.</p> <p>ППК-Р6.3. З-2. Знает принципы предметно-ориентированного проектирования (ПОП) программного обеспечения.</p> <p>ППК-Р6.3. З-3. Знает паттерны проектирования и антипаттерны.</p> <p>ППК-Р6.3. У-1. Умеет разрабатывать модульный и тестируемый программный код.</p> <p>ППК-Р6.3. У-2. Умеет выполнять модульное, интеграционное и нагрузочное тестирование.</p>                                                                                                                                                                                                                                              |

|                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                   | <p>ППК-Р6.3. У-3. Умеет проводить рефакторинг для повышения качества кода.</p> <p>ППК-Р6.3. У-4. Умеет применять принципы ПОП при разработке программного обеспечения на языках программирования высокого уровня абстракций и в LowCode и NoCode системах.</p>                                                                                                                                                                                                                                     |
|                                                                                                   | <p>ППК-Р6.4. Участвует в развертывании и поддержке программного обеспечения (продвинутой)</p> <p>ППК-Р6.4. З-1. Знает стратегии развертывания промышленного программного обеспечения.</p> <p>ППК-Р6.4. З-2. Знает основы работы с облачными платформами.</p> <p>ППК-Р6.4. У-1. Умеет развертывать приложения в облаке.</p> <p>ППК-Р6.4. У-2. Умеет обнаруживать и устранять инциденты с работой продуктивного программного обеспечения.</p>                                                        |
| ППК-Р7. Способен применять искусственный интеллект (ИИ) для генерации и отладки программного кода | <p>ППК-Р7.1. Применяет ИИ-инструменты для генерации программного кода (базовый)</p> <p>ППК-Р7.1. З-1. Знает принципы работы современных генеративных ИИ-моделей для генерации кода.</p> <p>ППК-Р7.1. З-2. Знает ограничения и риски использования ИИ-генерации (безопасность, качество кода, лицензирование).</p> <p>ППК-Р7.1. У-1. Умеет формулировать корректные текстовые запросы (промты) для генерации кода.</p> <p>ППК-Р7.1. У-2. Умеет интегрировать ИИ-инструменты в среду разработки.</p> |
|                                                                                                   | <p>ППК-Р7.2. Использует ИИ для анализа и отладки кода (средний)</p> <p>ППК-Р7.2. З-1. Знает методы ИИ-анализа кода.</p> <p>ППК-Р7.2. З-2. Знает форматы и инструменты для автоматизированного тестирования с ИИ.</p> <p>ППК-Р7.2. У-1. Умеет настраивать ИИ-инструменты для поиска уязвимостей.</p> <p>ППК-Р7.2. У-2. Умеет интерпретировать рекомендации ИИ по исправлению кода.</p>                                                                                                              |
|                                                                                                   | <p>ППК-Р7.3. Оптимизирует код с помощью ИИ (продвинутой)</p> <p>ППК-Р7.3. З-1. Знает методы ИИ-оптимизации.</p> <p>ППК-Р7.3. З-2. Знает критерии качества кода, применяемые ИИ-системами.</p> <p>ППК-Р7.3. У-1. Умеет использовать ИИ для рефакторинга.</p> <p>ППК-Р7.3. У-2. Умеет проверять корректность оптимизаций, предложенных ИИ.</p>                                                                                                                                                       |
|                                                                                                   | <p>ППК-Р7.4. Оценивает этические и профессиональные аспекты применения ИИ в разработке (продвинутой)</p> <p>ППК-Р7.4. З-1. Знает этические нормы использования ИИ (конфиденциальность, плагиат кода и т.п.).</p> <p>ППК-Р7.4. З-2. Знает лицензионные ограничения сгенерированного кода.</p> <p>ППК-Р7.4. У-1. Умеет проверять код на соответствие стандартам после ИИ-генерации.</p> <p>ППК-Р7.4. У-2. Умеет документировать использование ИИ в разработке.</p>                                   |
|                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ППК-ДА4. Способен выявлять бизнес-проблемы или бизнес-возможности                      | ППК-ДА4.2. Выявление истинных бизнес-проблем или бизнес-возможностей (продвинутый)<br>ППК-ДА4.2. 3-1. Знает предметную область и специфику деятельности организации в объеме, достаточном для решения задач бизнес-анализа<br>ППК-ДА4.2. 3-2. Знает инструменты, техники анализа бизнес-ситуации и предметной области, включая анализ данных.<br>ППК-ДА4.2. 3-3. Знает перспективные и существующие цифровые технологии и цифровые возможности для бизнеса в контексте предметной области и специфики деятельности организации.                                                                                                                              |
| РГ-1. Способен руководить процессами разработки компьютерного программного обеспечения | РГ-1.1. Руководит разработкой программного кода (средний)<br>РГ-1.1. 3-1. Знает методы принятия управленческих решений.<br>РГ-1.1. 3-2. Знает основные принципы и методы управления персоналом<br>РГ-1.1. 3-1 Знает технологии межличностной и групповой коммуникации в деловом взаимодействии, основы конфликтологии<br>РГ-1.1. У-1. Способен распределять задачи на разработку программного кода между исполнителями.<br>РГ-1.1. У-2. Применяет лучшие мировые практики оформления программного кода.<br>РГ-1.1. У-3. Оценивает качество и эффективность программного кода.                                                                                |
|                                                                                        | РГ-1.2. Руководит проверкой работоспособности компьютерного программного обеспечения (средний)<br>РГ-1.2. 3-1. Знает основные методы измерения и оценки характеристик компьютерного программного обеспечения<br>РГ-1.2. 3-2. Знает методы и средства проверки работоспособности компьютерного программного обеспечения<br>РГ-1.2. 3-3. Знает методы и средства рефакторинга и оптимизации программного кода<br>РГ-1.2. У-1. Умеет распределять задачи на проверку работоспособности компьютерного программного обеспечения между исполнителями.<br>РГ-1.2. У-2. Умеет оценивать результаты проверки работоспособности компьютерного программного обеспечения |
|                                                                                        | РГ-1.3. Руководит интеграцией программных модулей и компонентов компьютерного программного обеспечения (продвинутый)<br>РГ-1.3. 3-2. Знает методы и программные интерфейсы взаимодействия компьютерного программного обеспечения с внешними программными компонентами<br>РГ-1.3. 3-3. Знает методы проектирования и разработки программных интерфейсов взаимодействия внутренних модулей компьютерного программного обеспечения<br>РГ-1.3. У-1. Умеет назначать задания на разработку процедур интеграции, сборку, подключение к внешней среде, проверку работоспособности выпусков программного продукта                                                    |
| РГ-4. Способен организовать промышленную разработку программного обеспечения           | РГ-4.1. Внедряет промышленные методологии разработки (средний)<br>РГ-4.1. 3-1. Знает принципы Agile и их применение в промышленных проектах.<br>РГ-4.1. 3-2. Знает процессы code review, принципы                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|  |                                                                                                                                                                                                                                                                                                                             |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>коллективного владения кодом (collective code ownership).</p> <p>РГ-4.1. У-1. Умеет оценивать объем задач и срок их выполнения.</p> <p>РГ-4.1. У-2. Умеет распределять задачи между участниками команды.</p> <p>РГ-4.1. У-3. Умеет организовать работу в команде с использованием инструментов управления проектами.</p> |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### 3. Тематический план

| №п/<br>п                                  | Наименование<br>раздела дисциплины<br>(модуля)                 | Трудоемкость, академические часы |                          |          |                               | ТКУ<br>(текущий контроль<br>успеваемости) |
|-------------------------------------------|----------------------------------------------------------------|----------------------------------|--------------------------|----------|-------------------------------|-------------------------------------------|
|                                           |                                                                | Очная форма                      |                          |          |                               |                                           |
|                                           |                                                                | Аудиторная работа                |                          | Контроль | Самостояте<br>льная<br>работа |                                           |
|                                           |                                                                | Лекции                           | Практически<br>е занятия |          |                               |                                           |
| 1                                         | Современный<br>защищённый канал и<br>модель угроз              | 4                                | 4                        |          | 20                            | Домашнее задание<br>1                     |
| 2                                         | Идентичность,<br>подписи и<br>классическая<br>асимметрия       | 4                                | 4                        | 4        | 20                            | Домашнее задание<br>2                     |
| 3                                         | Защита данных: хеши,<br>шифрование,<br>целостность             | 8                                | 8                        | 4        | 20                            | Домашнее задание<br>2                     |
| 4                                         | Доверие в протоколах:<br>PKI, TLS 1.3, ECC                     | 6                                | 6                        |          | 30                            | Домашнее задание<br>1                     |
| 5                                         | Криптография в<br>инфраструктуре и<br>национальных<br>профилях | 2                                | 2                        | 4        | 36                            | Домашнее задание<br>1                     |
|                                           | Зачет с оценкой                                                |                                  |                          | 4        |                               | Проект                                    |
| Итого:                                    |                                                                | 24                               | 24                       | 16       | 126                           |                                           |
| Объем дисциплины (модуля)<br>(в ак. ч.)   |                                                                | 190                              |                          |          |                               |                                           |
| Объем дисциплины (модуля)<br>(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<br>(издания, курса, документа)                            | Ссылка                                                                          |
|----|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| 1. | Научная электронная библиотека elibrary.ru библиотека                          | <a href="https://elibrary.ru/defaultx.asp">https://elibrary.ru/defaultx.asp</a> |
| 2. | База данных для IT-специалистов                                                | <a href="https://habr.com">https://habr.com</a>                                 |
| 3. | База данных ScienceDirect                                                      | <a href="https://www.sciencedirect.com">https://www.sciencedirect.com</a>       |
| 4. | Официальный сайт Министерства науки и высшего образования Российской Федерации | <a href="https://minobrnauki.gov.ru/">https://minobrnauki.gov.ru/</a>           |
| 5. | Федеральный портал «Российское образование»                                    | <a href="https://www.edu.ru/">https://www.edu.ru/</a>                           |
| 6. | Информационная система "Единое окно доступа к образовательным ресурсам"        | <a href="http://window.edu.ru/">http://window.edu.ru/</a>                       |
| 7. | Единая коллекция цифровых образовательных ресурсов                             | <a href="http://school-collection.edu.ru/">http://school-collection.edu.ru/</a> |
| 8. | Федеральный центр информационно - образовательных ресурсов                     | <a href="http://fcior.edu.ru/">http://fcior.edu.ru/</a>                         |

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

|                                                                     |               |                           |
|---------------------------------------------------------------------|---------------|---------------------------|
| <b>Средства антивирусной защиты:</b>                                |               |                           |
| Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition | отечественное | лицензионное              |
| <b>Среды разработки:</b>                                            |               |                           |
| 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 |
| <b>Пакеты программных средств и библиотек:</b>                      |               |                           |
| AutoPsy                                                             | зарубежное    | свободно распространяемое |
| Interactive Disassembler (IDA)                                      | зарубежное    | свободно распространяемое |
| <b>Системы управления библиографической информацией:</b>            |               |                           |
| Zotero                                                              | зарубежное    | свободно распространяемое |
| <b>Сервисы и службы:</b>                                            |               |                           |
| 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 удастся, 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»:** « $0,24 \times \text{среднее за домашние задания 1} + 0,44 \times \text{среднее за домашние задания 2} + 0,32 \times \text{зачет с оценкой}$ ».

### **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)**

| №<br>п/п | Задание                                                                                                                                    | Ответ                                                                                                                                   | Компетенция   | Индикатор         |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------------|
| 1        | Опишите роли участников команды при разработке криптографического модуля и распределении задач по реализации протоколов.                   | Разработчик пишет код шифрования, криптограф проектирует алгоритмы, тестировщик проверяет уязвимости, все несут ответственность за этап | УК-3, УК-1    | УК-3.1, УК-1.2    |
| 2        | Как мотивировать команду и распределить ресурсы при реагировании на криптографические уязвимости с ограниченным временем?                  | Четкое распределение задач, контроль сроков, пример профессионализма, оценка трудоемкости этапов проекта                                | УК-3, РГ-1    | УК-3.2, РГ-1.2    |
| 3        | Подготовьте презентацию результатов аудита криптографической защиты для стейкхолдеров и руководства компании.                              | Структура: цель, методы, результаты, выводы, рекомендации с учетом целевых установок заинтересованных сторон                            | УК-1, ППК-ДА3 | УК-1.3, ППК-ДА3.2 |
| 4        | Оформите документацию по проекту криптографической системы согласно профессиональным стандартам и требованиям к техническим спецификациям. | Титульный лист, содержание, введение, основная часть, выводы, список источников, приложения по ГОСТ                                     | УК-1, ППК-Р5  | УК-1.3, ППК-Р5.3  |
| 5        | Дайте определение RSA-шифрованию и запишите её смысл в контексте асимметричной криптографии.                                               | RSA это алгоритм асимметричного шифрования основанный на сложности факторизации больших чисел для защиты данных                         | УК-1, ОПК-6   | УК-1.2, ОПК-6.1   |
| 6        | Проанализируйте экономическую информацию для выбора между алгоритмами шифрования для защищённого канала связи.                             | Сравнение затрат, производительности, рисков, учет специфики задач, влияние на эффективность бизнес-решений                             | УК-1, ОПК-6   | УК-1.2, ОПК-6.2   |
| 7        | Обоснуйте экономическое решение о выборе криптографического протокола на основе анализа затрат и выгод.                                    | Решение выбирается если учитывает интересы всех                                                                                         | УК-1, ОПК-6   | УК-1.3, ОПК-6.3   |

|    |                                                                                                                                  |                                                                                                                                      |                |                    |
|----|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|----------------|--------------------|
|    |                                                                                                                                  | сторон, повышает защиту инвестора от неблагоприятных изменений                                                                       |                |                    |
| 8  | Запишите формулу для оценки стойкости ключа и выберите метод анализа данных для криптоанализа.                                   | Формула стойкости зависит от длины ключа и алгоритма, метод статистического анализа для оценки значимости уязвимостей                | ОПК-6, ППК-ДА3 | ОПК-6.2, ППК-ДА3.2 |
| 9  | Оптимизируйте выбор криптографического алгоритма и обоснуйте влияние на бизнес показатели компании.                              | Выбор алгоритма с максимальной эффективностью, оценка воздействия на ключевые показатели компании, скорость обработки данных         | ОПК-6, ППК-Р5  | ОПК-6.3, ППК-Р5.3  |
| 10 | Обоснуйте экономическое решение в учебном проекте с учетом системного мышления при проектировании криптографической архитектуры. | Использование модели с учетом взаимосвязей между компонентами, ключами и бизнес-целями компании                                      | ОПК-6, РГ-4    | ОПК-6.3, РГ-4.1    |
| 11 | Назовите правовые нормы регулирующие использование криптографии в РФ и их смысл для проекта.                                     | ФЗ-63 Об электронной подписи, требования к сертификации СКЗИ, ответственность за нарушение требований при использовании криптографии | ППК-Р5, УК-1   | ППК-Р5.3, УК-1.1   |
| 12 | Примените правовые нормы при оценке рисков нарушения требований при работе с криптографическими средствами в организации.        | Анализ рисков несоблюдения законодательных требований, оценка вероятности и пороговых значений, меры минимизации штрафов             | ППК-Р5, ППК-Р6 | ППК-Р5.3, ППК-Р6.3 |
| 13 | Дайте правовую оценку ситуации с нарушением требований по защите данных в проекте криптографической системы.                     | Определение нарушений законодательных актов, применение санкций, влияние на репутацию организации                                    | ППК-Р5, УК-1   | ППК-Р5.3, УК-1.3   |

|    |                                                                                                                                   |                                                                                                                                        |                  |                      |
|----|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|------------------|----------------------|
| 14 | Выберите метод статистического анализа для проверки гипотез о влиянии изменений на стойкость криптографической системы.           | А/В тест, проверка гипотез о значимости различий, расчет доверительных интервалов для оценок времени взлома                            | ППК-ДА3, ППК-ДА4 | ППК-ДА3.2, ППК-ДА4.2 |
| 15 | Адаптируйте аналитическую модель оценки криптографических параметров под бизнес потребности и оцените влияние решений.            | Перевод технических метрик в бизнес показатели, оценка воздействия на ключевые показатели компании, оптимизация процессов безопасности | ППК-ДА3, ППК-Р6  | ППК-ДА3.2, ППК-Р6.3  |
| 16 | Выберите тип визуализации для представления данных о результатах аудита безопасности и коммуникации с руководством.               | График уровня защиты и доверительных интервалов, интерактивный дашборд для публичной дискуссии о результатах анализа                   | ППК-ДА3, УК-1    | ППК-ДА3.2, УК-1.3    |
| 17 | Выявите бизнес проблему на основе анализа отклонений в показателях криптографической защиты и примите решение.                    | Проблема низкой стойкости шифрования, выбор стратегии реагирования, решение о корректировке алгоритмов или конфигурации                | ППК-ДА4, ППК-Р7  | ППК-ДА4.2, ППК-Р7.2  |
| 18 | Классифицируйте бизнес возможности при масштабировании криптографической инфраструктуры с учетом стратегического планирования.    | Оптимизация вычислительных ресурсов, разработка плана действий с учетом целей компании, выявление резервов роста                       | ППК-ДА4, РГ-4    | ППК-ДА4.2, РГ-4.4    |
| 19 | Сформулируйте рекомендации на основе статистических выводов о результатах тестирования криптоалгоритмов для управления продуктом. | При значимом улучшении внедрение изменения, при отсутствии эффекта отказ от изменения для эффективности системы безопасности           | ППК-Р6, ППК-Р7   | ППК-Р6.3, ППК-Р7.3   |

|    |                                                                                            |                                                                                                            |            |                |
|----|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|------------|----------------|
| 20 | Оцените риски реализации проекта криптографической системы и разработайте меры управления. | Анализ вероятности срывов сроков, мониторинг индикаторов успешности, пересмотр плана при выявлении проблем | РГ-1, УК-1 | РГ-1.3, УК-1.3 |
|----|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|------------|----------------|