



АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
"ЕВРАЗИЙСКАЯ АКАДЕМИЯ"

УТВЕРЖДАЮ
Ректор
_____ **Замелый А.Ю./**



"05" июня 2025 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Криптография и криптографические алгоритмы»**

Дополнительная профессиональная программа
«Информационные и коммуникационные технологии»

г. Москва
Территория Инновационного центра Сколково

Наименование учебной дисциплины: Криптография и криптографические алгоритмы.

Цель освоения учебной дисциплины: достижение запланированных результатов освоения образовательной программы - формирование установленных в образовательной программе компетенций.

Задачи освоения учебной дисциплины: достижение запланированных в настоящей рабочей программе результатов освоения дисциплин - приобретение обучающимся запланированных знаний, умений, навыков.

Планируемые результаты освоения учебной дисциплины

Обучающийся должен сформировать следующие результаты освоения дисциплины «Криптография и криптографические алгоритмы»:

Знания: Знает математические основы криптографии, включая теорию чисел, алгебру, теорию вероятностей и математическую статистику. Знает историю развития криптографии и основные этапы ее эволюции. Знает современные тенденции развития криптографии, такие как квантовая криптография и постквантовая криптография.

Умения: Владеет навыками применения криптографических методов для защиты информации в различных системах и приложениях. Владеет навыками анализа и оценки безопасности криптографических систем. Владеет навыками использования специализированного программного обеспечения для криптографического анализа.

Навыки: Умеет применять математические методы для анализа и разработки криптографических алгоритмов. Умеет проводить сравнительный анализ различных криптографических алгоритмов и протоколов. Умеет разрабатывать простые криптографические протоколы для решения конкретных задач.

Объем (трудоемкость) учебной дисциплины: определен в учебном плане образовательной программы.

Форма промежуточной аттестации по учебной дисциплине определена в учебном плане образовательной программы.

Текущий контроль успеваемости осуществляется посредством аналитического отчета обучающегося по дисциплине.

Структура и содержание учебной дисциплины определяется тематическим планом учебной дисциплины.

Тематический план учебной дисциплины

Тема № 1: Введение в криптографию

Тема № 2: Симметричное шифрование

Тема № 3: Алгоритм DES

Тема № 4: Алгоритм AES

Тема № 5: Режимы работы блочных шифров

Тема № 6: Асимметричное шифрование

Тема № 7: Алгоритм RSA
Тема № 8: Алгоритм ECC
Тема № 9: Гибридные криптосистемы
Тема № 10: Хэш-функции
Тема № 11: Цифровые подписи
Тема № 12: Инфраструктура открытых ключей (PKI)
Тема № 13: Управление ключами
Тема № 14: Криптографические протоколы
Тема № 15: Протокол TLS/SSL
Тема № 16: Протокол SSH
Тема № 17: Криптография в блокчейне
Тема № 18: Криптовалюты и их безопасность
Тема № 19: Квантовая криптография
Тема № 20: Постквантовая криптография
Тема № 21: Атаки на криптографические системы
Тема № 22: Криптоанализ
Тема № 23: Дифференциальный криптоанализ
Тема № 24: Линейный криптоанализ
Тема № 25: Атаки на хэш-функции
Тема № 26: Атаки на цифровые подписи
Тема № 27: Безопасность веб-приложений
Тема № 28: Криптография в операционных системах
Тема № 29: Криптография в базах данных
Тема № 30: Криптография в облачных технологиях
Тема № 31: Криптографические библиотеки
Тема № 32: Стандарты криптографии
Тема № 33: Правовые аспекты криптографии
Тема № 34: Этические аспекты криптографии
Тема № 35: Будущее криптографии
Тема № 36: Практикум по симметричному шифрованию
Тема № 37: Практикум по асимметричному шифрованию
Тема № 38: Практикум по хэш-функциям и цифровым подписям

Содержание самостоятельной работы обучающихся по учебной дисциплине: подготовка к занятиям: изучение теоретического материала, чтение учебников и дополнительных источников, конспектирование; подготовка к промежуточной аттестации; самостоятельное изучение дополнительных материалов; анализ и интерпретация данных – составление аналитического отчета обучающегося по дисциплине.

Условия реализации рабочей программы дисциплины

Материально-техническое обеспечение реализации дисциплины соответствует материально-техническому обеспечению, указанному в разделе 3 образовательной программы.

Учебно-методическое обеспечение (электронные учебно-методические материалы) освоения учебной дисциплины

Электронные учебные издания

Куклина, Е. Н. Организация самостоятельной работы студента / Е. Н. Куклина, М. А. Мазниченко, И. А. Мушкина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 235 с. — (Высшее образование). — ISBN 978-5-534-06270-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/562503>

Зорина, Е. М. Метапредметная компетенция преподавателей и обучающихся / Е. М. Зорина. — Москва : Издательство Юрайт, 2025. — 130 с. — (Высшее образование). — ISBN 978-5-534-17997-2. — Текст : электронный // Образовательная платформа Юрайт [сайт].

Электронные методические издания

Мотивация студентов к обучению и воспитательная деятельность — Москва : Издательство Юрайт, 2023. — 1 с. — (Юрайт.Академия). — ISBN 978-5-534-14536-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/533252>

Мотивация студентов к обучению и профессиональному развитию — Москва : Издательство Юрайт, 2022. — 5 с. — (Юрайт.Академия). — ISBN 978-5-534-14536-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/509597>

Информационное обеспечение освоения учебной дисциплины представляет собой перечень информационных технологий, используемых при осуществлении образовательного процесса, включая перечень программного обеспечения и информационных справочных систем.

Каждый обучающийся обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной системе (цифровой (электронной) библиотеке) «ЮРАЙТ» (<https://urait.ru/>), содержащей издания учебно-методической и иной литературы.

Каждый обучающийся обеспечивается индивидуальным неограниченным доступом к федеральной государственной информационной системе «Национальная электронная библиотека» (<https://rusneb.ru/>).

Состав необходимого комплекта лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства: Яндекс Браузер (реестровая запись №3722 от 23.07.2017 в едином реестре российских программ для электронных вычислительных машин и баз данных); Яндекс.Телемост (реестровая запись №13556 от 20.05.2022 в едином реестре российских программ для электронных вычислительных машин и баз данных)

Электронные информационные ресурсы (ресурсы информационно-телекоммуникационной сети «Интернет»):

- Состав современных профессиональных баз данных

Федеральная служба государственной статистики (<https://rosstat.gov.ru/>)

Открытые данные России (<https://data.gov.ru/>)

Статистический Отдел Организации Объединенных Наций (United Nations Statistics Division) (<http://data.un.org/>)

База данных ЮНЕСКО (<https://www.unesco.org/en/key-data>)

- Состав информационных справочных систем

База знаний Открытого правительства (<http://wiki.ac-forum.ru/>)

Высшая аттестационная комиссия при Министерстве науки и высшего образования Российской Федерации (<https://vak.minobrnauki.gov.ru/main>)

Российский фонд фундаментальных исследований (<https://www.rfbr.ru/>)

Официальный интернет-портал правовой информации (Государственная система правовой информации) (<http://pravo.gov.ru/>)

Система обеспечения законодательной деятельности (<https://sozd.duma.gov.ru/>)

Собрание законодательства Российской Федерации (<https://www.szrf.ru/>)

Государственная автоматизированная система Российской Федерации «Правосудие» (ГАС «Правосудие») (<https://sudrf.ru/>)

Нормативные правовые акты в Российской Федерации. Министерство юстиции Российской Федерации (<http://pravo.minjust.ru/>)

- Иные информационные ресурсы - информационные ресурсы органов государственной власти

Президент России (<http://kremlin.ru/>)

Правительство России (<http://government.ru/>)

Министерство науки и высшего образования РФ (<https://www.minobrnauki.gov.ru/>)

Министерство просвещения РФ (<https://edu.gov.ru/>)

Министерство экономического развития Российской Федерации (<https://www.economy.gov.ru/>)

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (<https://digital.gov.ru/>)

- Иные информационные ресурсы - периодическими издания

ТАСС (<https://tass.ru/>)

РИА НОВОСТИ (<https://ria.ru/>)

Коммерсантъ (<https://www.kommersant.ru/>)

RT (<https://rt.com/>)

- Информационные поисковые системы

Яндекс (<https://ya.ru/>)

MAIL.RU (<https://www.mail.ru/>)