

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИНГУШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФИЗИКО- МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра «Информационные системы и технологии»**

СОГЛАСОВАНО

Руководитель образовательной программы

_____/М.Х.Мальсагов
от «27» апреля 2026г.

УТВЕРЖДАЮ

Декан физико-математического
факультета

_____/ М.Х.Мальсагов
от «28» апреля 2026г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.04. Криптографические методы защиты информации

Направление подготовки

09.03.02 Информационные системы и технологии

Направленность (профиль подготовки)

Безопасность информационных систем

Квалификация выпускника

Бакалавр

Форма обучения

Очная, заочная

Магас, 2026г

1. Цели освоения дисциплины

Дисциплина "Криптографические методы защиты информации" содержит основные положения криптографии, знакомит с наиболее распространенными типами шифров и методами их криптоанализа, понятиями целостности информации, криптографическими протоколами, электронной подписью. Объясняется математическая теория, лежащая в основе криптографии (теория групп, полей Галуа, неприводимые многочлены, теория чисел, псевдослучайные последовательности и др.). Ставятся вопросы реализации алгоритмов шифрования и криптоанализа

2. Место дисциплины в структуре ОПОП бакалавриата

Цикл, к которому относится дисциплина:

Б1.В.04. «Криптографические методы защиты информации»

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	Код	Наименование	Уровень квалификации	Наименование	Код	Уровень (подуровень) квалификации
06.026 Системный администратор информационно-коммуникационных систем	D	Обслуживание серверных операционных систем информационно-коммуникационной системы	6	Выполнение работ по выявлению и устранению нетипичных инцидентов, возникающих в серверных операционных системах информационно-коммуникационной системы	D/01.6	6
				Проведение анализа и определение основных причин сложных проблем, возникающих на серверах и в серверных операционных системах	D/02.6	6
				Выполнение планирования резервного копирования, архивирования и восстановления конфигурации серверов и серверных операционных систем	D/03.6	6
				Планирование изменений параметров работы серверов и серверных операционных систем	D/04.6	6

			Выполнение обновления программного обеспечения серверных операционных систем	D/05.6	6
			Прогнозирование влияния внешних и внутренних воздействий на поведение серверных операционных систем	D/06.6	6
			Прогнозирование потребности в изменении объемов необходимых ресурсов для обеспечения бесперебойной работы серверов и серверных операционных систем	D/07.6	6
			Планирование и проведение работ по распределению нагрузки между имеющимися ресурсами, снятию нагрузки на серверы и серверные операционные системы перед проведением регламентных работ, восстановлению штатной схемы работы в случае сбоев	D/08.6	6
			Определение потребностей в приобретении специализированных средств контроля и тестирования серверов и серверных операционных систем	D/09.6	6

Данная учебная дисциплина включена осваивается на 4 курсе, 7 семестр. Дисциплина из цикла Профессиональный. Студент должен владеть дисциплинами общепрофессионального цикла, уметь: понимать, излагать и критически анализировать базовую общефизическую информацию; использовать математический аппарат, использовать навыки экспериментальной работы; владеть дисциплинами Профессионального цикла, должен знать основные мероприятия по организационно-правовому обеспечению информационной безопасности; как осуществляются программно-аппаратные средства защиты информации; основные языки программирования. Основы информационной безопасности, Безопасность вычислительных сетей, Программно-аппаратные средства защиты информации, Теоретические основы компьютерной безопасности

могут рассматриваться как предшествующие дисциплины. Знания и навыки, полученные при изучении дисциплины Криптографические методы защиты информации будут использованы при работе над курсовыми и дипломными проектами и диссертациями.

**Связь дисциплины «Криптографические методы защиты информации»
»
с предшествующими дисциплинами и сроки их изучения**

Код дисциплины	Дисциплины, предшествующие дисциплине «Криптографические методы защиты информации»	Семестр
Б1.В.04.	Основы криптографии	5

3. Результаты освоения дисциплины (модуля) «Криптографические методы защиты информации»

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
ПК-5	ПК-5 - Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ИК- 5.1 формирует модель угроз и определяет криптографические меры защиты с учётом ФСТЭК 77/239 ИК- 5.2 проводит крипто-стойкостной анализ конфигурации (выбор алгоритмов, ключевых длин) и проверку соответствия ГОСТам. ИК- 5.3 готовит полный пакет аттестационной документации (программа-	Знать • порядок аттестации объектов информатизации (Приказ ФСТЭК № 77) перечень допустимых криптоалгоритмов и ключевых длин (ГОСТы, NIST SP 800-175B) -место криптографии в задаче информационной безопасности и построения защищенных

		методика, акт испытаний, заключение). информационных систем ; -основные понятия теории криптографии - классические исторические шифры и методы атак на эти шифры, современные шифры - криптографические протоколы и электронную подпись; - типичные слабости реализации криптографических систем (PGP, RC4, Windows и др.); - теоретические основы "хорошего" шифра по Шеннону; - теоретические основы "хорошей" криптосистемы (правила Кирхгоффа) Уметь - выбирать СКЗИ, составлять программу испытаний, проводить хеш- и ЭЦП-контроль (ГОСТ 34.11-2012) - правильно выбирать тип шифра в соответствии с поставленной задачей ; - качественно реализовать алгоритм шифрования; - реализовывать атаку на классические шифры (исторические и современные) Владеть средствами автоматизированной проверки соответствия (SCAP-сканеры, CryptoPro TLS) и навыками подготовки отчётных форм ФСТЭК математические основы криптографии (неприводимые многочлены, теория чисел, псевдо-случайные последовательности
--	--	---

СП1.5	Подготовка к лабораторным работам	10
СП1.6	Подготовка к рубежному контролю	12
СП1.7	Другие виды самостоятельной работы	10

5. Образовательные технологии

В процессе преподавания Модуля используются следующие методы, средства и обновляемое при необходимости программное обеспечение информационных технологий:

- e-mail преподавателя;
- электронные учебно-методические материалы для обеспечения самостоятельной работы студентов;
- список сайтов в сети «Интернет» для поиска научно-технической информации по разделам дисциплины;
- Комплект из OpenSSL, CryptoPro CSP, PyCryptodome, libsodium, SoftHSM, HashiCorp Vault, Wireshark, testssl.sh, SSLyze, Hashcat (плюс OpenSC и CI-инструменты)

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Для обеспечения самостоятельной работы студентов по Модулю сформирован методический комплекс, включающий в себя следующие учебно-методические материалы:

1. Программа курса.
2. Учебники и учебные пособия.
3. Список адресов сайтов в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), содержащих актуальную информацию по блокам Модуля.

Библиографические ссылки на учебные издания, входящие в методический комплекс, приведены в перечне основной и дополнительной учебной литературы, необходимой для освоения Модуля (раздел 7).

К дополнительным материалам также относится перечень ресурсов сети «Интернет», рекомендуемых для самостоятельной работы при освоении Модуля (раздел 7). Студенты получают доступ к указанным материалам на первом занятии по Модулю.

7. Учебно-методическое и материально-техническое обеспечение дисциплины(модуля)

7.1. Учебная литература:

Основная литература по модулю

1. **Васильева И. Н.** *Криптографические методы защиты информации: учебник и практикум для академического бакалавриата.* — М.: Юрайт, 2020. — 349 с.
2. **Аграновский А. В., Хади Р. А.** *Практическая криптография: алгоритмы и их программирование.* — М.: СОЛОН-Пресс, 2009. — 256 с.
3. **Гатченко Н. А., Исаев А. С., Яковлев А. Д.** *Криптографическая защита информации.* — СПб.: НИУ ИТМО, 2012. — 142 с.

Дополнительные учебные материалы

1. *Основы криптографии.* Учебное пособие, 2-е изд. — М.: Гелиос АРВ, 2002. — 480 с.

2. Токарева О. А. Симметричная криптография. Краткий курс. PDF-конспект спецкурса Новосибирского государственного университета, 2020.

3. Варлатая С. К., Шаханова М. В. Криптографические методы и средства обеспечения информационной безопасности. — М.: Проспект, 2023. — 152 с.

4. Столлингс У. Криптография и защита сетей. Принципы и практика. Пер. с англ. — М.: Вильямс, 2019. — 912 с.

7.2. Интернет-ресурсы

Примерный перечень ресурсов сети «интернет», рекомендуемых при освоении модуля

1. **PyCryptodome Docs** — подробные примеры кода AES, HMAC и KDF на Python; студенты используют их в домашних заданиях. pycryptodome.readthedocs.io
2. **CryptoPro CSP** — официальный портал загрузок и PDF-инструкций для реализации ГОСТ-алгоритмов и TLS с отечественными криптопараметрами. cryptopro.rucryptopro.ru
- 3.

7.3. Программное обеспечение:

- Microsoft Windows 7, Windows 8, Windows 8.1, Windows 10
- Microsoft Windows server 2003, 2008, 2012, 2016
- Microsoft Office 2007, 2010, 2016
- VS Code
- OpenSSL, CryptoPro CSP
-

7.4. Материально-техническое обеспечение

Описание материально-технической базы, необходимой для изучения модуля

Перечень материально-технического обеспечения Модуля

№ п/п	Вид занятий	Вид и наименование оборудования
1	Лекционные занятия	Аудитории с мультимедийными средствами, средствами звуковоспроизведения и имеющие выход в сеть «Интернет». Помещения для проведения аудиторных занятий, оборудованные учебной мебелью
2	Лабораторные работы	Компьютерный класс с комплексом программных средств, позволяющих каждому студенту разрабатывать программные реализации практических задач в ходе выполнения лабораторных работ
3	Самостоятельная работа	Библиотека, имеющая рабочие места для студентов. Аудитории, оснащенные компьютерами с доступом к сети «Интернет»
4	Практика	Компьютерный класс с комплексом программных средств, позволяющих каждому студенту разрабатывать программные реализации практических задач в ходе выполнения лабораторных работ

Рабочая программа дисциплины «Криптографические методы защиты информации» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02 «Информационные системы и технологии», утвержденного приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 г. № 926(ред.8.02.2021).

Программу составил:

К.педаг.наук, старший преподаватель кафедры «Информационные системы и технологии» Ажигов А.М

Программа одобрена на заседании кафедры «Информационные системы и технологии»

Протокол № 8 от «27» апреля 2026 года

Программа одобрена Учебно-методической комиссией физико-математического факультета

Протокол №6 от «28» апреля 2026 года

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата)	Внесенные изменения	Подпись зав. кафедрой

Приложение

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В. 04. Криптографические методы защиты информации

Направление подготовки

09.03.02 Информационные системы и технологии

Направленность (профиль подготовки)

Безопасность информационных систем

Квалификация выпускника

Бакалавр

Форма обучения

Очная, заочная

Магас, 2026г

ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Фонд оценочных средств (ФОС) предусматривает следующее:

- описание комплекса **показателей** – дескрипторов освоения компетенций в виде результатов обучения, которые студент может продемонстрировать (
- (таблица 1). Для контроля достижения каждого из них предусмотрены оценочные средства в виде вопросов, заданий и т.д.;
- обозначение **критериев** – правил принятия решения по оценке достигнутых результатов обучения и сформированности компетенций.

Например, в качестве шкалы оценивания принимается 100-балльная система с выделением (градацией) оценок:

Рейтинг	Оценка на зачете
85–100	Зачет
71–84	
60–70	
0–59	Незачет

ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИЕ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Выпускник, освоивший образовательную программу, должен обладать профессиональными компетенциями по тематическим модулям программы:

Код	Наименование тематического модуля	Результаты обучения
	Введение в искусственный интеллект и основные методы машинного обучения для работы с табличными данными	Знания: – теоретические основы анализа данных и машинного обучения; – специфика работы алгоритмов машинного обучения. Умения: - применение методов машинного обучения, подготовка данных и интерпретация результатов. Навыки (опыт деятельности): - интересуется новыми трендами в своей профессиональной отрасли, рассматривает их с точки зрения применения в своей деятельности; - оценивает применимость алгоритмов, возможные риски и последствия ошибок, находит оптимальные решения для рабочих задач

	Системы глубокого обучения	Знания: - принципы обучения и применения нейронных сетей. - архитектуры глубоких нейронных сетей, применяемых в решении практических задач связанных с анализом изображений и текстов; Умения: - настройка необходимого окружения для работы с нейронными сетями. - применение и дообучениепредобученных нейронных сетей из доступных библиотек Навыки (опыт деятельности): - владеет навыком проведения полного цикла вычислительного эксперимента, отражения хода выполнения проекта и получения результатов в отчетах и документации; - владеет навыком использования существующих программных библиотек и моделей, создания программных реализаций глубоких нейронных сетей
	Обучение с подкреплением	Знания: - теоретические основы и алгоритмы обучения с подкреплением; - применение обучения с подкреплением для практических задач. Умения: - выбор и реализация алгоритмов обучения с подкреплением с учетом специфики задачи - адаптация и настройка алгоритмов обучения с подкреплением под определенную среду. Навыки (опыт деятельности): - интересуется новыми трендами в своей профессиональной отрасли, рассматривает их с точки зрения применения в своей деятельности; - владеет навыком использования существующих программных библиотек и моделей, создания программных реализаций на основе алгоритмов обучения с подкреплением

Средства для оценки различных уровней формирования компетенций по категориям «знать», «уметь», «владеть» обеспечивают реализацию основных принципов контроля, таких как объективность и независимость, практико-ориентированность, междисциплинарность.

С учетом этого контрольные вопросы (задания, задачи), входящие в ФОС, для различных категорий и уровней освоения компетенций могут иметь следующий вид.

ЗНАТЬ Примеры:

1. Типы задач машинного обучения и классы алгоритмов, к ним применяемые.
2. Основные направления развития исследований в области систем искусственного интеллекта.
3. Теоретические основы алгоритмов машинного обучения.

УМЕТЬ Примеры:

1. Подготовить данные к использованию алгоритма машинного обучения.
2. Оценивать качество решений систем машинного обучения.
3. Адаптировать алгоритмы машинного обучения к решению практических задач.

ВЛАДЕТЬ Примеры:

1. Методология разработки решений машинного обучения.
2. Примеры практического применения архитектур искусственного интеллекта.
3. Методы онлайн тестирования решений машинного обучения.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИЕ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Примеры (макеты) методических материалов, определяющих процедуры оценивания знаний, умений и (или) опыта деятельности

Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Текущий контроль успеваемости	Средство проверки освоения уровней «знать», «уметь» компетенций	Комплекты билетов (заданий)

Комплект билетов (примерный)

Билет 1.

- 1.1 Опишите структуру раунда и ключевые размеры блочного шифра **AES**.
- 1.2 Как режим **GCM** обеспечивает одновременно конфиденциальность и аутентификацию данных?

Билет 2.

- 2.1 Перечислите особенности алгоритма **ГОСТ 28147-89** (сеть Фейстеля, длина блока/ключа).
- 2.2 Сравните режимы работы ECB, CBC и CTR с точки зрения параллелизма и утечек шаблона

Билет 3.

- 3.1 Опишите этапы генерации ключей и принцип работы **RSA**.
- 3.2 Назовите шаги формирования и проверки ЭЦП по **ГОСТ 34.10-2012**.

Билет 4.

- 4.1 Покажите упрощённый handshake протокола **TLS 1.3** и объясните механизм Perfect Forward Secrecy
- 4.2 Как утилита **testssl.sh** помогает выявлять слабые шифронаборы на сервере?

Билет 5.

- 5.1 Чем конструкция **SHA-3 (FIPS 202)** отличается от SHA-2 и какую роль играет «губка» (sponge)?
- 5.2 Перечислите основные параметры (t, m, p) функции хеширования паролей **Argon2id** и их влияние на стойкость.

Билет 6.

- 6.1 Раскройте математическую основу **секретного разделения Шамира** и схемы (k, n).

6.2 Опишите жизненный цикл криптографического ключа по NIST SP 800-175B (создание → уничтожение)..

Билет 7.

7.1 Что такое интерфейс **PKCS#11** и как **SoftHSM v2** эмулирует аппаратный HSM?
7.2

Объясните алгоритм **HMAC** и его доказанную связь с стойкостью базовой хеш-функции

Перечень лабораторных работ (примерный)

Общие рекомендации к лабораторным работам: для разных уровней подготовки студентов можно использовать разную глубину реализации решения. Так, для студентов нетехнических специальностей задание может заключаться в применении готовых методов из библиотек или заполнением пропусков в программах, где большая часть подготовлена преподавателем. Для студентов технических специальностей задание будет заключаться в реализации алгоритмов без использования готовых решений.

ЛР1.1 Методы работы с таблицами в Python. Агрегация и визуализация данных. Проведение первичного анализа данных.

Цели: изучение методов работы с данными в Python и проведение первичного анализа данных.

Задание: загрузите датасет в pandas-датафрейм. Выведите основные параметры датасета. Определите, сколько в датасете случаев отсутствия признаков. Определите, сколько признаков являются категориальными. Визуализируйте распределение признаков по классам. Визуализируйте зависимость между признаками.

ЛР1.2 Использование и сравнение алгоритмов классификации: kNN, решающие деревья и их ансамбли, логистическая регрессия.

Цели: применение и оценка алгоритмов классификации.

Задание:

Разделите датасет на обучающий и валидационный с сохранением пропорций классов. Классифицируйте точки из датасета с помощью алгоритмов kNN, логистической регрессии, CART, случайного леса, CatBoost. Подберите лучшие параметры алгоритмов с помощью валидационной выборки. Сравните время работы алгоритмов и зависимость от предобработки данных.

ЛР1.3 Использование и оценка алгоритмов регрессии. Подбор оптимальных параметров регрессии.

Цели: изучение алгоритмов регрессии.

Задание:

Примените метод линейной регрессии для решения задачи на датасете. Добавьте в датасет полиномиальные признаки. Добавляйте признаки пока не увидите переобучение на валидационном датасете. Примените гребневую регрессию и LASSO, чтобы избавиться от переобучения.

ЛР1.4 Оптимизационные задачи и их решения. Подбор гиперпараметров алгоритма с помощью методов оптимизации

Цели: изучение алгоритмов решения оптимизационных задач.

Задание:

1. Оптимизируйте длину маршрута в задаче комивояжера с помощью алгоритмов hillclimb, отжига и генетического алгоритма. Выведите получившийся путь и его длину.
2. Оптимизируйте гиперпараметры алгоритма машинного обучения (на выбор) с помощью случайного поиска, поиска по решетке, алгоритма hillclimb, генетического алгоритма.

ЛР2.1 Классификация изображений и трансферное обучение.

Цели: изучение методов глубокого обучения для работы с изображениями.

Задание:

Загрузите датасет и создайте итератор для модели глубокого обучения. Загрузите предобученную на ImageNet сверточную сеть (AlexNet, VGG или ResNet) и добавьте к backbone полносвязный слой для обучения. Обучите нейронную сеть на, визуализировав график функции потерь на обучающей и валидационной выборке. Реализуйте модуль применения нейронной сети к данным, проверьте качество обучения на тестовой выборке.

ЛР2.2 Работа с текстами и их векторными представлениями. Цели:

изучение моделей векторного представления текстов. Задание:

Скачайте предобученные вектора для словаря. С помощью любого классификатора машинного обучения (kNN, SVM, CatBoost) классифицируйте тексты из датасета по сумме векторов слов. Классифицируйте тексты с помощью LSTM сети.

ЛР3. 1 Применение Q-Networks для решения простых окружений.

Цели: изучение применения обучения с подкреплением для решений задач контроля.

Задание:

Обучите простую полносвязную Q-сеть для решения окружения LunarLander.

Процедуры оценивания знаний, умений, формы и организация текущего контроля успеваемости и промежуточной аттестации обучающихся

Текущий контроль успеваемости и промежуточная аттестация студентов ведется в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации образовательной организации

Текущий контроль успеваемости

Модуль делится на два блока. Каждый блок включает в себя изучение законченного раздела, части Модуля.

Текущий контроль по Модулю осуществляется по календарному учебному графику. Сроки контрольных мероприятий (КМ) и сроки подведения итогов по Модулю отображаются в рабочих учебных планах на семестр. Студент должен выполнить все контрольные мероприятия, предусмотренные Модулем к указанному сроку, после чего преподаватель проставляет балльные оценки, набранные студентом по результатам текущего контроля успеваемости по Модулю.

Контрольное мероприятие считается выполненным, если за него студент получил оценку в баллах не ниже минимальной оценки, установленной программой модуля по данному мероприятию.

Студенты, не сдавшие контрольное мероприятие в установленный срок, продолжают работать над ним в соответствии с порядком, принятым образовательной организацией.

Промежуточная аттестация

Формой промежуточной аттестации по Модулю является зачет.

Оценивание Модуля ведется в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации студентов образовательной организации.

Например, методика оценки по рейтингу

Студент, выполнивший все предусмотренные учебным планом задания и сдавший все контрольные мероприятия, получает итоговую оценку по Модулю за семестр в соответствии со следующей шкалой:

Рейтинг	Оценка на зачете
85-100	Зачет
71-84	
60-70	
0-59	Незачет

Рейтинг студента по Модулю за семестр определяется как сумма баллов, полученных им за все блоки Модуля, и баллов за промежуточную аттестацию. Максимальное количество баллов за Модуль в семестре устанавливается равным 100