МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский ядерный университет «МИФИ»
Институт интеллектуальных кибернетических систем

**2384**

# Учебный план основной образовательной программы

## Теоретическая и практическая криптография

**по направлению 10.04.01 «Информационная безопасность»**

**Уровень:** Магистратура
**Квалификация:** магистр
очная форма обучения
2024 год приема

УМС ИИКС НИЯУ МИФИ.
Протокол №8/1/2023 от 28.08.2023

## 1. График учебного процесса

| | Сентябрь | | | | | Октябрь | | | | Ноябрь | | | | Декабрь | | | | | Январь | | | | Февраль | | | | Март | | | | | Апрель | | | | Май | | | | Июнь | | | | | Июль | | | | Август | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1-7 сент. | 8-14 сент. | 15-21 сент. | 22-28 сент. | 29 сент.-5 окт. | 6-12 окт. | 13-19 окт. | 20-26 окт. | 27 окт. - 2 нояб. | 3-9 нояб. | 10-16 нояб. | 17-23 нояб. | 24-30 нояб. | 1-7 дек. | 8-14 дек. | 15-21 дек. | 22-28 дек. | 29 дек.-4 янв. | 5-11 янв. | 12-18 янв. | 19-25 янв. | 26 янв.-1 фев. | 2-8 февр. | 9-15 февр. | 16-22 февр. | 23 фев. - 1 марта | 2-8 марта | 9-15 марта | 16-22 марта | 23-29 марта | 30 марта-5 апр. | 6-12 апр. | 13-19 апр. | 20-26 апр. | 27 апр.-3 мая | 4-10 мая | 11-17 мая | 18-24 мая | 25-31 мая | 1-7 июня | 8-14 июня | 15-21 июня | 22-28 июня | 29 июня-5 июля | 6-12 июля | 13-19 июля | 20-26 июля | 27 июля- 2 авг. | 3-9 авг. | 10-16 авг. | 17-23 авг. | 24-30 авг. |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 |
| Годы 1 | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | | Э | Э | Э | К | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Э | Э | Э | Э | К | К | К | К | К | К | К | К |
| Годы 2 | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | | Э | Э | Э | К | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Т | Э | Э | П | П | П | П | Д | Д | Д | Д | К | К | К | К | К | К | К | К |

Т — теоретическое обучение, Э — экзаменационная сессия, К — каникулы, П — практика, Д — выпускная квалификационная работа

# 2. План учебного процесса

| Метка | Название | Структурное подразделение | ЗЕТ | ч | Семестры | | | | | | | | | | | | | | | | | | | | | | | | Практическая подготовка | Компетенции |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 курс | | | | | | | | | | | | 2 курс | | | | | | | | | | | | | |
| | | | | | 1 *18 нед* (ТО: 18 нед) | | | | | | 2 *17 нед* (ТО: 17 нед) | | | | | | 3 *18 нед* (ТО: 18 нед) | | | | | | 4 *11 нед* (ТО: 11 нед) | | | | | | | |
| | | | | | Ауд | Лек | Пр | Лаб | СРС | Атт | Ауд | Лек | Пр | Лаб | СРС | Атт | Ауд | Лек | Пр | Лаб | СРС | Атт | Ауд | Лек | Пр | Лаб | СРС | Атт | | |
| **Б1** | **Дисциплины (модули)** | | **69** | **2484** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Б1.ОД** | **Базовая часть** | | **15** | **540** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Б1.ОД.1** | **Общенаучный модуль** | | **7** | **252** | **64** | **16** | **48** | | **80** | | **30** | | **30** | | **42** | | | | | | | | | | | | | | | |
| Б1.ОД.1.1 **О** | Иностранный язык (специальный курс) | 50 | 5 | 180 | 32 | | 32 | | 40 | *З* | 30 | | 30 | | 42 | *Э(36)* | | | | | | | | | | | | | | УК-4, УК-5 |
| Б1.ОД.1.2 **О** | Методология и организация научных исследований | 41 | 2 | 72 | 32 | 16 | 16 | | 40 | *З* | | | | | | | | | | | | | | | | | | | | УК-1, УК-6, ОПК-4, ОПК-5, ПК-1, ПК-2, ПК-3, УКЦ-1, УКЦ-2 |
| **Б1.ОД.2** | **Профессиональный модуль** | | **8** | **288** | | | | | | | **120** | **60** | **45** | **15** | **132** | | | | | | | | | | | | | | | |
| Б1.ОД.2.1 **О** | Защищенные информационные системы (Protected Information Systems) | 44 | 4 | 144 | | | | | | | 60 | 30 | 15 | 15 | 48 | *Э(36)* | | | | | | | | | | | | | | УК-2, УК-6, ОПК-1, ОПК-2, ПК-1, ПК-2 |
| Б1.ОД.2.2 **О** | Управление информационной безопасностью | 44 | 4 | 144 | | | | | | | 60 | 30 | 30 | | 84 | *З/О, К/р* | | | | | | | | | | | | | | УК-1, УК-3, ОПК-3, ПК-1, ПК-2 |
| **Б1.ДВ** | **Вариативная часть** | | **54** | **1944** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Б1.ДВ.1** | **Общенаучный модуль** | | **15** | **540** | **192** | **96** | **96** | | **96** | | **45** | **15** | **30** | | **27** | | **64** | **32** | **32** | | **8** | | | | | | | | | |
| Б1.ДВ.1.1 **Ф** | Методы дискретной математики в криптографии | 41 | 3 | 108 | 64 | 32 | 32 | | 8 | *Э(36)* | | | | | | | | | | | | | | | | | | | | ПК-1, ПК-3, ПК-5.2 |
| Б1.ДВ.1.2 **Ф** | Основы квантовой информатики | 41 | 2 | 72 | | | | | | | 45 | 15 | 30 | | 27 | *З* | | | | | | | | | | | | | | ПК-1, ПК-2, ПК-3, УКЦ-1 |
| Б1.ДВ.1.3 **Ф** | Алгебраические основы криптографии | 41 | 4 | 144 | 64 | 32 | 32 | | 44 | *Э(36), К/р* | | | | | | | | | | | | | | | | | | | | ПК-2, УКЦ-2, ПК-5.2 |
| Б1.ДВ.1.4 **Ф** | Методы теории вероятностей и математической статистики в криптографии | 41 | 4 | 144 | 64 | 32 | 32 | | 44 | *Э(36)* | | | | | | | | | | | | | | | | | | | | ПК-1, ПК-3, УКЦ-1 |
| Б1.ДВ.1.5 **Ф** | Эллиптические кривые в криптографии | 41 | 2 | 72 | | | | | | | | | | | | | 64 | 32 | 32 | | 8 | *З* | | | | | | | | ПК-1, ПК-3, УКЦ-2 |
| **Б1.ДВ.2** | **Профессиональный модуль** | | **39** | **1404** | **144** | **112** | | **32** | **108** | | **135** | **75** | **60** | | **117** | | **224** | **128** | **64** | **32** | **244** | | **105** | **30** | **45** | **30** | **75** | | | |
| Б1.ДВ.2.1 **Ф** | Асимметричные криптосистемы | 42 | 4 | 144 | 64 | 64 | | | 44 | *Э(36)* | | | | | | | | | | | | | | | | | | | | ПК-1, ПК-3, УКЦ-1, ПК-5.2 |
| Б1.ДВ.2.2 **Ф** | Симметричные криптосистемы (Symmetric Cryptosystems) | 41 | 4 | 144 | | | | | | | 60 | 30 | 30 | | 48 | *Э(36), К/р* | | | | | | | | | | | | | | ПК-1, УКЦ-1, УКЦ-2, ПК-5.1, ПК-5.2 |
| Б1.ДВ.2.3 **Ф** | Квантовая криптография | 41 | 2 | 72 | | | | | | | | | | | | | 32 | 16 | 16 | | 40 | *З* | | | | | | | | ПК-1, УКЦ-2 |
| Б1.ДВ.2.4 **Ф** | Современные криптосистемы | 41 | 3 | 108 | | | | | | | | | | | | | 32 | 16 | 16 | | 40 | *Э(36), К/п* | | | | | | | | ПК-2, ПК-3, УКЦ-2, ПК-5.2 |

| Метка | Название | Структурное подразделение | ЗЕТ | ч | Семестры | | | | | | | | | | | | | | | | | | | | | | | | Практическая подготовка | Компетенции |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 курс | | | | | | | | | | | | 2 курс | | | | | | | | | | | | | |
| | | | | | 1 *18 нед* (ТО: 18 нед) | | | | | | 2 *17 нед* (ТО: 17 нед) | | | | | | 3 *18 нед* (ТО: 18 нед) | | | | | | 4 *11 нед* (ТО: 11 нед) | | | | | | | |
| | | | | | Ауд | Лек | Пр | Лаб | СРС | Атт | Ауд | Лек | Пр | Лаб | СРС | Атт | Ауд | Лек | Пр | Лаб | СРС | Атт | Ауд | Лек | Пр | Лаб | СРС | Атт | | |
| Б1.ДВ.2.5 Ф | *Б1.ДВ.2.5.1* Методы построения деструктивных воздействий *Б1.ДВ.2.5.2* Основы методов оптимизации в машинном обучении | 41 | 2 | 72 | | | | | | | | | | | | | 32 | 16 | | 16 | 40 | *З* | | | | | | | — | УКЦ-1, ПК-5.2 |
| Б1.ДВ.2.6 Ф | Основы криптоанализа | 41 | 3 | 108 | | | | | | | | | | | | | 48 | 32 | 16 | | 24 | *Э(36)* | | | | | | | | ПК-1, УКЦ-1, ПК-5.1, ПК-5.2 |
| Б1.ДВ.2.7 Ф | *Б1.ДВ.2.7.1* Практическое применение криптографических протоколов *Б1.ДВ.2.7.2* Современные модели кибератак | 41 | 3 | 108 | | | | | | | | | | | | | | | | | | | 45 | 15 | 30 | | 27 | *Э(36)* | — | УК-1, УКЦ-2, ПК-5.2 |
| Б1.ДВ.2.8 Ф | *Б1.ДВ.2.8.1* Криптографические протоколы *Б1.ДВ.2.8.2* Дополнительные разделы низкоуровневого программирования | 42 / 12 | 5 | 180 | | | | | | | 30 | 15 | 15 | | 42 | *З* | 32 | 16 | 16 | | 40 | *Э(36)* | | | | | | | — | УКЦ-1, ПК-5.1, ПК-5.2 |
| Б1.ДВ.2.9 Ф | *Б1.ДВ.2.9.1* Основы теории дискретной информации и кодирования *Б1.ДВ.2.9.2* Мультипарадигмальное программирование | 41 | 2 | 72 | | | | | | | 45 | 30 | 15 | | 27 | *З* | | | | | | | | | | | | | — | УКЦ-1, УКЦ-2 |
| Б1.ДВ.2.10 Ф | *Б1.ДВ.2.10.1* Архитектуры современных операционных систем *Б1.ДВ.2.10.2* Современные методы программирования в задачах информационной безопасности | 41 | 2 | 72 | 48 | 32 | | 16 | 24 | *З* | | | | | | | | | | | | | | | | | | | — | УКЦ-1, УКЦ-2 |
| Б1.ДВ.2.11 Ф | Введение в методы динамического анализа программного обеспечения | 41 | 2 | 72 | 32 | 16 | | 16 | 40 | *З* | | | | | | | | | | | | | | | | | | | | УКЦ-1, УКЦ-2 |
| Б1.ДВ.2.12 Ф | Технология обеспечения информационной безопасности объектов | 44 | 3 | 108 | | | | | | | | | | | | | 48 | 32 | | 16 | 60 | *З/О, К/р* | | | | | | | | ПК-1, ПК-3, УКЦ-1 |
| Б1.ДВ.2.13 Ф | *Б1.ДВ.2.13.1* Прикладная информационная безопасность *Б1.ДВ.2.13.2* Прикладная стеганография и стеганоанализ | 41 | 4 | 144 | | | | | | | | | | | | | | | | | | | 60 | 15 | 15 | 30 | 48 | *Э(36)* | — | УКЦ-2, ПК-5.1, ПК-5.2 |
| **Б2** | **Практика** | | **45** | **1620** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Б2.ОД** | **Базовая часть** | | **11** | **396** | | | | | | | | | | | | | | | | | | | | | | | | | | |

| Метка | Название | Структурное подразделение | ЗЕТ | ч | Семестры | | | | | | | | | | | | | | | | | | | | | | | | Практическая подготовка | Компетенции |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 курс | | | | | | | | | | | | 2 курс | | | | | | | | | | | | | |
| | | | | | 1 *18 нед* (ТО: 18 нед) | | | | | | 2 *17 нед* (ТО: 17 нед) | | | | | | 3 *18 нед* (ТО: 18 нед) | | | | | | 4 *11 нед* (ТО: 11 нед) | | | | | | | |
| | | | | | Ауд | Лек | Пр | Лаб | СРС | Атт | Ауд | Лек | Пр | Лаб | СРС | Атт | Ауд | Лек | Пр | Лаб | СРС | Атт | Ауд | Лек | Пр | Лаб | СРС | Атт | | |
| Б2.ОД.1 О | Производственная практика (получение профессиональных умений и опыта профессиональной деятельности) | 41 | 11 | 396 | | | | | | | | | | | | | | | | | | | 22 | | | | 338 | *Э(36)* | 30 | УК-1, УК-2, УК-3, УК-6, ОПК-3, ОПК-4, ОПК-5, ПК-1, ПК-2 |
| **Б2.ДВ** | **Вариативная часть** | | **34** | **1224** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Б2.ДВ.1 Ф | Производственная практика (научно-исследовательская работа) | 41 | 28 | 1008 | 96 | | | | 192 | *З/О* | 30 | | | | 222 | *Э(36)* | 32 | | | | 364 | *Э(36)* | | | | | | | 200 | УК-1, УК-4, УК-6, ПК-2, ПК-3, ПК-5.1, ПК-5.2 |
| Б2.ДВ.2 Ф | Производственная практика (преддипломная) | 41 | 6 | 216 | | | | | | | | | | | | | | | | | | | | | | | 216 | *З/О* | 216 | ПК-1, ПК-2, ПК-3, УКЦ-1, УКЦ-2, ПК-5.1, ПК-5.2 |
| **Б3** | **Государственная итоговая аттестация** | | **6** | **216** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Б3.1 О | Подготовка к процедуре защиты и защита выпускной квалификационной работы | 41 | 6 | 216 | | | | | | | | | | | | | | | | | | | | | | | 216 | | | УК-1, УК-2, УК-3, УК-4, УК-5, УК-6, ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5, ПК-1, ПК-2, ПК-3, УКЦ-1, УКЦ-2, ПК-5.1, ПК-5.2 |
| **Ф** | **Факультативы** | | **5** | **180** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Ф.1 Ф | Военная подготовка | 20 | 5 | 180 | | | | | | | | | | | | | | | | | | | | | | | | | | УК-1, УК-3, УК-6 |
| | | | | | **496** | **224** | **144** | **32** | **476** | | **360** | **150** | **165** | **15** | **540** | | **320** | **160** | **96** | **32** | **616** | | **127** | **30** | **45** | **30** | **845** | | | |
| | | | **Всего:** | **120 +5** | **4320 +180** | **31 ЗЕТ** | | | | | **29 ЗЕТ** | | | | | | **30 ЗЕТ** | | | | | | **30 ЗЕТ** | | | | | | **446 ч** | |
| | | | **Объем аудиторных занятий (ч/нед)** | | | **27.56** | | | | | **21.18** | | | | | | **17.78** | | | | | | **11.55** | | | | | | | |
| | | | **Максимальная учебная нагрузка (ч/нед)** | | | **54** | | | | | **52.94** | | | | | | **52** | | | | | | **49.09** | | | | | | | |
| | | | **Учебная нагрузка в сессию (ч/нед)** | | | **48** | | | | | **36** | | | | | | **48** | | | | | | **54** | | | | | | | |
| | | | **Зачет** | | | **4** | | | | | **3** | | | | | | **3** | | | | | | | | | | | | | |
| | | | **Зачет с оценкой** | | | **1** | | | | | **1** | | | | | | **1** | | | | | | **1** | | | | | | | |
| | | | **Экзамен** | | | **4** | | | | | **4** | | | | | | **4** | | | | | | **3** | | | | | | | |
| | | | **Курсовой проект** | | | | | | | | | | | | | | **1** | | | | | | | | | | | | | |
| | | | **Курсовая работа** | | | **1** | | | | | **2** | | | | | | **1** | | | | | | | | | | | | | |

**СОГЛАСОВАНО:**