

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ УНИВЕРСИТЕТ «МИФИ»**

УТВЕРЖДАЮ

Первый проректор НИЯУ МИФИ

_____ О.В. Нагорнов

« ____ » _____ 2018 г.

**КОМПЕТЕНТНОСТНАЯ МОДЕЛЬ ВЫПУСКНИКА,
ЗАВЕРШИВШЕГО ОБУЧЕНИЕ ПО ПРОГРАММЕ МАГИСТРАТУРЫ**

Направление подготовки
10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Программа подготовки
«Теоретическая и практическая криптография»

Квалификация:
Магистр

Длительность обучения
два года

Москва 2018

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Компетентностная модель соответствует требованиям образовательного стандарта НИЯУ МИФИ по направлению подготовки **10.04.01 Информационная безопасность** (квалификация (степень) «магистр»), образовательного стандарта НИЯУ МИФИ утвержден Ученым советом университета, протокол №13/06 от 07.11.2013г.

1.2. Основными пользователями компетентностной модели являются:

1.2.1 Объединения специалистов и работодателей в соответствующей сфере профессиональной деятельности.

1.2.2 Профессорско-преподавательские коллективы высших учебных заведений, ответственные за качественную разработку, эффективную реализацию и обновление основных образовательных программ с учетом достижений науки, техники и социальной сферы по данному направлению подготовки.

1.2.3 Студенты, осваивающие образовательную программу вуза, нацеленную на формирование данных компетенций.

1.2.4 Проректоры, отвечающие в пределах своей компетенции за качество подготовки выпускников.

1.3. Компетентностная модель является основой для проектирования содержания основной образовательной программы магистратуры «Теоретическая и практическая криптография».

2 ГЛОССАРИЙ

В настоящем документе используются термины и определения в соответствии с Федеральным законом РФ «Об образовании в Российской Федерации», а также с международными документами в сфере высшего образования:

вид профессиональной деятельности – методы, способы, приемы, характер воздействия на объект профессиональной деятельности с целью его изменения, преобразования;

компетенция – способность применять знания, умения и личностные качества для успешной деятельности в определенной области;

направление подготовки – совокупность образовательных программ различного уровня в одной профессиональной области;

объект профессиональной деятельности – системы, предметы, явления, процессы, на которые направлено воздействие;

область профессиональной деятельности – совокупность объектов профессиональной деятельности в их научном, социальном, экономическом, производственном проявлении.

В настоящем документе используются следующие сокращения:

ВО – высшее образование;

КМ – компетентностная модель;

ОК – общекультурные компетенции;

ОПК – общепрофессиональные компетенции;

ПК – профессиональные компетенции.

3 КОМПЕТЕНТНОСТНАЯ МОДЕЛЬ

3.1. Цели ВО по магистерской программе «Теоретическая и практическая криптография» в области обучения и воспитания личности.

3.1.1. В области обучения целью ВО по магистерской программе является: получение выпускниками профессиональных компетенций, необходимых для выполнения должностных обязанностей, связанных с применением методов криптологии для обеспечения безопасности информации, хранимой и/или обрабатываемой на критически важных объектах, в том числе в ядерной отрасли и других отраслях народного хозяйства.

3.1.2. В области воспитания личности целью ВО по магистерской программе является развитие у студентов личностных качеств, а также формирование общекультурных (универсальных, общенаучных, социально-личностных, инструментальных и др.) и профессиональных компетенций в соответствии с требованиями ФГОС ВО по направлению подготовки **10.04.01 Информационная безопасность** (квалификация (степень) «магистр»).

3.2. Область профессиональной деятельности выпускников

Область профессиональной деятельности выпускников по магистерской программе «Теоретическая и практическая криптография» включает сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением информационной безопасности и защиты информации критически важных объектов в организациях высокотехнологических отраслей.

Обучение по данной магистерской программе частично удовлетворяет потребности в кадрах со стороны организаций, обладающих информационно-технологическими ресурсами, подлежащими защите с помощью методов, средств и технологий, базирующихся на криптографии.

3.3. Объекты профессиональной деятельности выпускников

Объектами профессиональной деятельности выпускника по магистерской программе «Теоретическая и практическая криптография» являются:

фундаментальные и прикладные проблемы информационной безопасности;

объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы в организациях высокотехнологических отраслей;

средства и технологии обеспечения информационной безопасности и защиты информации;

экспертиза, сертификация и контроль защищенности информации и критически важных объектов в организациях высокотехнологических отраслей;

методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности критически важных объектов в организациях высокотехнологических отраслей;

организация и управление информационной безопасностью;

образовательный процесс в области информационной безопасности.

3.4. Виды профессиональной деятельности выпускников

Виды профессиональной деятельности выпускника по магистерской программе «Теоретическая и практическая криптография»:

проектная;
научно-исследовательская и инновационная;
контрольно-аналитическая;
педагогическая;
организационно-управленческая.

3.5. Задачи профессиональной деятельности выпускников

Задачи профессиональной деятельности выпускника:

а) проектная деятельность:

системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности, согласованных со стратегией развития информационных систем критически важных объектов в организациях высокотехнологических отраслей;

обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

разработка систем, комплексов, средств и технологий обеспечения информационной безопасности критически важных объектов в организациях высокотехнологических отраслей;

разработка программ и методик испытаний средств и систем обеспечения информационной безопасности критически важных объектов в организациях высокотехнологических отраслей;

б) научно-исследовательская деятельность:

анализ фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества;

разработка планов и программ проведения научных исследований и технических разработок, подготовка отдельных заданий для исполнителей;

выполнение научных исследований с применением соответствующих физических и математических методов;

подготовка по результатам научных исследований отчетов, статей, докладов

на научных конференциях;

в) контрольно-аналитическая деятельность:

аудит информационной безопасности информационных систем и объектов информатизации критически важных объектов в организациях высокотехнологических отраслей;

аттестация объектов информатизации критически важных объектов в организациях высокотехнологических отраслей по требованиям безопасности информации;

г) педагогическая деятельность:

выполнение учебной (преподавательской) и методической работы в организациях, осуществляющих образовательную деятельность, по дисциплинам (модулям) соответствующих профилю подготовки;

д) организационно-управленческая деятельность:

организация работы коллектива исполнителей, принятие управленческих решений, определение порядка выполнения работ;

организация управления информационной безопасностью критически важных объектов в организациях высокотехнологических отраслей;

организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации (далее – ФСБ России), Федеральной службы по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК России);

организация и выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности критически важных объектов в организациях высокотехнологических отраслей;

разработка проектов организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности критически важных объектов в организациях высокотехнологических отраслей.

3.6. Требования к результатам освоения основной образовательной программы определяются отдельно для направления подготовки магистров по направлению 10.04.01 и дополнительно для магистерской программы «Теоретическая и практическая криптография».

Требования к результатам освоения основной образовательной программы определены на уровне формулирования компетенций.

Выпускник ВО по направлению 10.04.01 «Информационная безопасность» с квалификацией (степенью) «магистр» должен обладать общекультурными компетенциями (таблица 1), общепрофессиональными компетенциями (таблица 2), профессиональными (по видам профессиональной деятельности) компетенциями (таблица 3). Выпускник ВО по магистерской программе «Теоретическая и практическая криптография» (направление 10.04.01 «Информационная безопасность») должен обладать дополнительными профессиональными компетенциями (таблица 4).

Таблица 1. Общекультурные компетенции выпускника по направлению 10.04.01 «Информационная безопасность»

ОБЩЕКУЛЬТУРНЫЕ КОМПЕТЕНЦИИ		
№	Код компетенции	Выпускник должен обладать следующими общекультурными компетенциями:
1.	ОК-1	способность к абстрактному мышлению, анализу, синтезу
2.	ОК-2	способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения

Таблица 2. Общепрофессиональные компетенции выпускника по направлению 10.04.01 «Информационная безопасность»

ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ		
№	Код компетенции	Выпускник должен обладать следующими общепрофессиональными компетенциями:
3.	ОПК-1	способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности
4.	ОПК-2	способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности

Таблица 3. Профессиональные компетенции выпускника по направлению 10.04.01 «Информационная безопасность»

ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ ПО ВИДАМ ДЕЯТЕЛЬНОСТИ		
№	Код компетенции	Выпускник должен обладать следующими профессиональными компетенциями:
<i>проектная деятельность:</i>		
5.	ПК-1	способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты
6.	ПК-2	способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности
7.	ПК-3	способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов
8.	ПК-4	способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности
<i>научно-исследовательская деятельность:</i>		
9.	ПК-5	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества
10.	ПК-6	способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок
11.	ПК-7	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента
12.	ПК-8	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи
<i>контрольно-аналитическая деятельность:</i>		
13.	ПК-9	способность проводить аудит информационной безопасности информационных систем и объектов информатизации

14.	ПК-10	способность проводить аттестацию объектов информатизации по требованиям безопасности информации
<i>педагогическая деятельность:</i>		
15.	ПК-11	способность проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности
<i>организационно-управленческая деятельность:</i>		
16.	ПК-12	способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения
17.	ПК-13	способность организовать управление информационной безопасностью
18.	ПК-14	способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России
19.	ПК-15	способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности
20.	ПК-16	способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности

Таблица 4. Дополнительные профессиональные компетенции выпускника по магистерской программе «Теоретическая и практическая криптография»

ДОПОЛНИТЕЛЬНЫЕ ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ		
№	Код компетенции	Выпускник должен обладать следующими дополнительными профессиональными компетенциями:
21.	ПСК-1	способность развивать математические, физические и/или технические методы криптографии
22.	ПСК-2	способность разрабатывать вычислительные алгоритмы, реализующие современные криптографические методы защиты информации
23.	ПСК-3	способность проводить анализ методов и алгоритмов, применяемых для защиты информации с помощью криптографических средств
24.	ПСК-4	способность обеспечивать эффективную криптографическую защиту информационно-технологических ресурсов организации

25.	ПСК-5	способность разрабатывать проектные решения по обеспечению информационной безопасности с применением криптографических методов, проводить анализ
26.	ПСК-6	способность проводить анализ компонентов систем безопасности с учетом современных и перспективных математических методов

**Директор института
интеллектуальных
кибернетических систем**

_____ /Мисюрин С.Ю./

**И.о. зав. кафедрой
«Криптология и
кибербезопасность»**

_____ /Елишкина А.В./

**Руководитель программы
д.ф.-м.н., доцент кафедры
«Криптология и
кибербезопасность»**

_____ /Пудовкина М.А./

СОГЛАСОВАНО:

Представители работодателей: