МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Ректор
_____ В.Д. Нечаев
«____» _____ 2023 г.

ПРИНЯТО
решением ученого совета
Севастопольского государственного университета
«___» _____ 2023 года
Протокол № _____

ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ

Направление подготовки
10.04.01 Информационная безопасность

Профиль
Управление информационной безопасностью в органах государственной власти

Квалификация
магистр

Форма обучения, год набора
очная, очно-заочная, 2023

Севастополь
2023

ЛИСТ СОГЛАСОВАНИЯ
Основной образовательной программы
высшего образования

Уровень высшего образования — **магистратура** (название)

Направление подготовки — **10.04.01 Информационная безопасность** (код и название)

Профиль — **Управление информационной безопасностью в органах государственной власти** (название)

Квалификация — **магистр** (название)

Проректор по образовательной деятельности _____ (подпись) _____ (дата) В.Р. Душко

Директор Дирекции развития образовательных программ _____ (подпись) _____ (дата) У.В. Дремова

Директор Института информационных технологий _____ (подпись) _____ (дата) В.Н. Бондарев

РАЗРАБОТАНО

Руководитель образовательной программы
д.т.н., доцент, профессор кафедры «Информационная безопасность» _____ (подпись) _____ (дата) Ю.Ю. Гончаренко

Лист согласования основной образовательной программы с представителями работодателей или их объединений в соответствующей области профессиональной деятельности

Основная образовательная программа высшего образования по направлению подготовки 10.04.01 Информационная безопасность (профиль: Управление информационной безопасностью в органах государственной власти, 2023 год набора) соответствует требованиям федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утверждённого приказом Министерства науки и высшего образования Российской Федерации от 26.11.2020 № 1455, отвечает требованиям профессиональных стандартов, соответствующих профессиональной деятельности выпускников, и требованиям к выпускникам на рынке труда.

	Рецензент (ведущий специалист – представитель работодателей или их объединений в соответствующей области профессиональной деятельности)
Основная образовательная программа по направлению подготовки 10.04.01 Информационная безопасность	Начальник Управления защиты государственной тайны и мобилизационной работы Правительства г. Севастополя (ученая степень, ученое звание, должность, место работы) _____ В.С. Кобизской *(подпись)* *(И.О. Фамилия)*
Программа государственной итоговой аттестации по направлению подготовки 10.04.01 Информационная безопасность	Начальник Управления защиты государственной тайны и мобилизационной работы Правительства г. Севастополя (ученая степень, ученое звание, должность, место работы) _____ В.С. Кобизской *(подпись)* *(И.О. Фамилия)*
Фонды оценочных средств государственной итоговой аттестации по направлению подготовки 10.04.01 Информационная безопасность	Начальник Управления защиты государственной тайны и мобилизационной работы Правительства г. Севастополя (ученая степень, ученое звание, должность, место работы) _____ В.С. Кобизской *(подпись)* *(И.О. Фамилия)*

СОДЕРЖАНИЕ

1. Общие положения

1.1. Определение образовательной программы высшего образования по направлению подготовки 10.04.01 Информационная безопасность.

Основная образовательная программа высшего образования – программа магистратуры по направлению подготовки 10.04.01 Информационная безопасность (профиль: Управление информационной безопасностью в органах государственной власти) (далее – основная образовательная программа), реализуемая в федеральном государственном автономном образовательном учреждении высшего образования «Севастопольский государственный университет» (далее – Университет), представляет собой систему документов, разработанную с учетом потребностей регионального рынка труда, на основе федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26.11.2020 № 1455 (далее – федеральный государственный образовательный стандарт высшего образования).

Основная образовательная программа представляет собой комплекс основных характеристик образования (объем, содержание, планируемые результаты), организационно-педагогических условий, форм аттестации, который представлен в виде: учебного плана, календарного учебного графика, рабочих программ дисциплин, программ практик, программы государственной итоговой аттестации, а также оценочных и методических материалов.

В настоящей программе используются следующие сокращения:

АИАД – автоматизация информационно-аналитической деятельности;

ДОТ – дистанционные образовательные технологии;

ЗТКС – защищенная телекоммуникационная система;

ИАС – информационно-аналитическая система;

НИОКР – научно-исследовательские и опытно-конструкторские работы;

НСД – несанкционированный доступ;

ООП – основная образовательная программа;

ОПК – общепрофессиональные компетенции;

ПК – профессиональные компетенции;

СКЗИ – средство криптографической защиты информации;

СССЭ – средства связи сетей электросвязи;

УК – универсальные компетенции;

ФГОС ВО – федеральный государственный образовательный стандарт высшего образования;

ЭИОС – электронная информационно-образовательная среда;

ЭО – электронное обучение.

1.2. Нормативные документы для разработки ООП

1.2.1. Настоящая основная образовательная программа разработана с учетом требований следующих нормативных правовых документов:

- Федерального Закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утверждённого приказом Министерства науки и высшего образования Российской Федерации от 26.11.2020 № 1455, зарегистрированного в Минюсте России 18 февраля 2021 г., рег. № 62549;
- Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования России от 6 апреля 2021 г. № 245;

- Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры, утвержденного приказом Министерства образования и науки Российской Федерации от 29.06.2015 № 636 (в ред. приказа Минобрнауки России от 9 февраля 2016 г. № 86, от 27 марта 2020 г. № 490);

- Положения о практической подготовке обучающихся, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 05.08.2020 № 885/390 (в ред. совместного приказа Министерства науки и высшего образования Российской Федерации и Минпросвещения России от 18 ноября 2020 года N 1430/652);

- Постановления Правительства РФ от 10 февраля 2014 № 92 «Об утверждении Правил участия объединений работодателей в мониторинге и прогнозировании потребностей экономики в квалифицированных кадрах, а также в разработке и реализации государственной политики в области среднего профессионального образования и высшего образования»;

- Письма Министерства образования и науки РФ № 03-956 от 13.05.2010 г. «Разъяснения разработчикам основных образовательных программ для реализации федеральных государственных образовательных стандартов высшего профессионального образования».

1.2.2. Настоящая основная образовательная программа разработана с учетом требований устава Университета, Положения о порядке разработки и утверждения основной образовательной программы № 42-01-09/281, принятого решением ученого совета Севастопольского государственного университета (протокол № 18 от 30.08.2022) и утвержденного приказом ректора от 31.08.2022 № 1731-п, иных локальных нормативных актов, действующих в Университете.

1.3. Общая характеристика ООП

Форма обучения ___очная, очно-заочная_____
(очная, очно-заочная, заочная)

Срок освоения ООП _____2 года, 2 года 5 месяцев_____

Профиль подготовки __Управление информационной безопасностью в органах государственной власти_____

Главной целью основной образовательной программы по направлению подготовки 10.04.01 «Информационная безопасность» является развитие у студентов личностных качеств, формирование универсальных, общепрофессиональных и профессиональных компетенций для решения задач проектной, научно-исследовательской, контрольно-аналитической, педагогической и организационно-управленческой деятельности в соответствии с требованиями ФГОС ВО и достижениями науки и техники в области информационной безопасности.

Миссия (социальная значимость) основной образовательной программы по направлению подготовки 10.04.01 «Информационная безопасность» состоит в концептуальном обосновании, моделировании современных условий и обеспечении подготовки высокопрофессиональных магистров, имеющих высокий теоретический и практический уровень непосредственно в области защиты информации и информационных технологий, и способных эффективно, с использованием фундаментальных теоретических и прикладных знаний и инновационных технологий осуществлять профессиональную деятельность в области информационной безопасности.

В области воспитания общей целью образовательной программы является создание условий по всестороннему развитию личности студентов, формирование социально-личностных и деловых качеств студентов: целеустремленности, организованности, трудолюбия, ответственности, гражданственности, коммуникативности, толерантности – позволяющих реализовать потенциал для решения профессиональных и социальных задач в профессиональной деятельности.

В области обучения общими целями образовательной программы по направлению подготовки 10.04.01 «Информационная безопасность» являются:

1) подготовка студентов в области основ гуманитарных, социальных, экономических, математических и естественнонаучных знаний и профессиональной деятельности;

2) получение высшего образования, позволяющего выпускнику успешно осуществлять решение задач профессиональной деятельности следующих типов:

- ***проектный***: системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности; 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; разработка программ и методик, испытаний средств и систем обеспечения информационной безопасности;

- ***научно-исследовательский***: 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;

- ***организационно-управленческий***: организация работы коллектива исполнителей, принятие управленческих решений, определение порядка выполнения работ; организация управления информационной безопасностью; 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; разработка проектов организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Согласно ФГОС ВО образовательная деятельность по программе магистратуры осуществляется на государственном (русском) языке Российской Федерации, если иное не определено локальным нормативным актом образовательной организации.

При успешном завершении обучения выпускнику присваивается квалификация «магистр» по специальности 10.04.01 «Информационная безопасность».

После успешного завершения обучения и профессиональной адаптации магистры по направлению подготовки 10.04.01 «Информационная безопасность» должны достичь следующих профессионально-ориентированных целей:

1) формирование способностей к самосовершенствованию и профессиональному росту;

2) готовность к ведению проектной, научно-исследовательской и организационно-управленческой деятельности;

3) умение сочетать теоретические знания и практические навыки для решения профессиональных задач.

1.4. Требования к уровню подготовки, необходимому для освоения ООП

Требования к уровню подготовки, необходимому для освоения ООП определяются Правилами приема в ФГАОУ ВО «Севастопольский государственный университет» на обучение по программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (далее - Правила), ежегодно устанавливаемыми решением ученого совета Севастопольского государственного университета. Правила приема представлены на

официальном сайте Университета в разделе «Правила приема» (https://www.sevsu.ru/admission/item/85-pravila-priema/) (прямая ссылка на Правила приема 2023 г. https://www.sevsu.ru/upload/iblock/446/y2o3p4ivwiyigle35nxdsov2lhh74032/Правила приема 2023.pdf).

Прием на обучение по направлению подготовки 10.04.01 «Информационная безопасность» проводится на базе высшего образования любого уровня – по результатам вступительных испытаний и с учетом среднего балла диплома.

2. Характеристика профессиональной деятельности выпускников

2.1. Общее описание профессиональной деятельности выпускников

Области профессиональной деятельности и (или) сфера (сферы) профессиональной деятельности выпускников, освоивших программу магистратуры по направлению подготовки 10.04.01 «Информационная безопасность», включают сферы образования и науки (профессионального образования и дополнительного профессионального образования, научных исследований, связанных с обеспечением информационной безопасности и защиты информации), связи, информационных и коммуникационных технологий (защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи, технической защиты информации, защиты значимых объектов критической информационной инфраструктуры (далее – ЗО КИИ), информационно-аналитических систем безопасности), обеспечения безопасности (обнаружения, предупреждения и ликвидации последствий компьютерных атак, криптографической защиты информации, эксплуатации технических и программно-аппаратных средств защиты информации, защиты значимых объектов КИИ, финансового мониторинга в целях противодействия легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма), иные техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере, а также другие области профессиональной деятельности и (или) сферы профессиональной деятельности при условии соответствия уровня их образования и полученных компетенций требованиям к квалификации работника.

Объектами профессиональной деятельности выпускников, освоивших программу магистратуры, являются:

- фундаментальные и прикладные проблемы информационной безопасности;
- объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы;
- средства и технологии обеспечения информационной безопасности и защиты информации; экспертиза, сертификация и контроль защищенности информации и объектов информатизации;
- методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации;
- организация и управление информационной безопасностью;
- образовательный процесс в области информационной безопасности.

Типы задач профессиональной деятельности, к решению которых готовятся выпускники, освоившие программу магистратуры:

- проектный;
- научно-исследовательский;
- организационно-управленческий.

ООП магистратуры ориентирована на все виды профессиональной деятельности, к которым готовится магистр.

2.2. Перечень профессиональных стандартов, соотнесенных с ФГОС ВО

Основная образовательная программа высшего образования – программа магистратуры по направлению подготовки 10.04.01 Информационная безопасность (профиль: Управление информационной безопасностью в органах государственной власти) разработана в соответствии с требованиями:

- Профессионального стандарта 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 03.11.2016 № 608н (зарегистрирован Министерством юстиции Российской Федерации 25.11.2016, регистрационный № 44449);
- Профессионального стандарта 06.031 «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 09.11.2016 № 611н (зарегистрирован Министерством юстиции Российской Федерации 22.11.2016, регистрационный № 44398);
- Профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 01.11.2016 № 598н (зарегистрирован Министерством юстиции Российской Федерации 28.11.2016, регистрационный № 44464);
- Профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15.09.2016 № 522н (зарегистрирован Министерством юстиции Российской Федерации 28.09.2016, регистрационный № 43857);
- Профессионального стандарта 06.034 «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 01.11.2016 № 599н (зарегистрирован Министерством юстиции Российской Федерации 28.09.2016, регистрационный № 44443).

Специалист по информационной безопасности должен выполнять обобщенные трудовые функции и трудовые функции, имеющие отношение к профессиональной деятельности, указанные в таблице 2.1.

Таблица 2.1

Область профессиональной деятельности (по Реестру Минтруда)	Обобщенная трудовая функция	Трудовая функция
Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи от несанкционированного доступа к ним (06.030)	Разработка средств защиты СССЭ (за исключением сетей связи специального назначения) от НСД	Анализ угроз информационной безопасности в сетях электросвязи
		Разработка средств и систем защиты СССЭ от НСД, защищенных телекоммуникационных систем (ЗТКС)
		Проведение научно-исследовательских и опытно-конструкторских работ (НИОКР) в сфере разработки средств и систем защиты СССЭ от НСД, создания ЗТКС
	Обеспечение защиты средств связи сетей связи специального назначения от НСД	Организация функционирования сетей связи специального назначения и их средств связи
		Проведение НИОКР в сфере разработки сетей связи специального назначения и их средств связи, включая СКЗИ
		Контроль защищенности от НСД и функциональности сетей связи специального назначения
	Управление развитием средств и систем защиты СССЭ от НСД	Управление рисками систем защиты сетей электросвязи от НСД
		Управление отношениями с поставщиками и потребителями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД
		Управление отношениями с регуляторами в сфере защиты информации
	Экспертиза проектных решений в сфере защиты СССЭ от НСД	Исследование эффективности способов, средств и систем защиты СССЭ от НСД
		Разработка технологических процессов производства программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД
Автоматизация информационно-аналитической деятельности (АИАД) в государственных	Применение ИАС в защищенном исполнении в процессах АИАД	Автоматизированная информационно-аналитическая поддержка процессов принятия

Область профессиональной деятельности (по Реестру Минтруда)	Обобщенная трудовая функция	Трудовая функция
органах, обеспечивающих национальную безопасность (06.031)		решений
		Решение типовых задач обработки информации в ИАС государственных органов, обеспечивающих национальную безопасность
		Решение типовых задач анализа информации в ИАС государственных органов, обеспечивающих национальную безопасность
	Проектирование ИАС в защищенном исполнении	Проведение предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений
		Выбор технологии и основных компонентов обеспечивающей части создаваемых ИАС
		Разработка проектных документов на создаваемые ИАС
		Проектирование обеспечивающей части ИАС
		Исследование эффективности ИАС
	Эксплуатация ИАС в защищенном исполнении	Настройка ИАС для решения задач в сфере профессиональной деятельности
		Обеспечение функционирования ИАС
		Обеспечение функционирования средств защиты информации в ИАС
	Организационное управление в ИАС в защищенном исполнении	Управление работой коллектива информационно-аналитических работников и специалистов по созданию и эксплуатации ИАС
		Разработка нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование ИАС
		Организация работ по выполнению в ИАС требований защиты информации ограниченного доступа

Область профессиональной деятельности (по Реестру Минтруда)	Обобщенная трудовая функция	Трудовая функция
	Проведение исследований в области эффективных технологий АИАД	Анализ и обобщение результатов научных исследований и разработок в области технологий АИАД
		Моделирование и исследование технологий АИАД
		Выработка и внедрение научно обоснованных решений, повышающих эффективность технологий АИАД
Защита информации в компьютерных системах и сетях (06.032)	Оценивание уровня безопасности компьютерных систем и сетей	Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации
		Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей
		Проведение анализа безопасности компьютерных систем
		Проведение сертификации программно-аппаратных средств защиты информации и анализ результатов
		Проведение инструментального мониторинга защищенности компьютерных систем и сетей
		Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов
	Разработка программно-аппаратных средств защиты информации компьютерных систем и сетей	Разработка требований к программно-аппаратным средствам защиты информации компьютерных систем и сетей
		Проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей
		Разработка и тестирование средств защиты информации компьютерных систем и сетей
		Сопровождение разработки средств защиты информации компьютерных систем и сетей
Обеспечение безопасности информации в автоматизированных системах (06.033)	Разработка систем защиты информации автоматизированных систем	Тестирование систем защиты информации автоматизированных систем
		Разработка проектных

Область профессиональной деятельности (по Реестру Минтруда)	Обобщенная трудовая функция	Трудовая функция
		решений по защите информации в автоматизированных системах
		Разработка эксплуатационной документации на системы защиты информации автоматизированных систем
		Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем
	Формирование требований к защите информации в автоматизированных системах	Обоснование необходимости защиты информации в автоматизированной системе
		Определение угроз безопасности информации, обрабатываемой автоматизированной системой
		Разработка архитектуры системы защиты информации автоматизированной системы
		Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации
Техническая защита информации (06.034)	Разработка средств защиты информации	Разработка технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок
		Разработка технических средств защиты акустической речевой информации от утечки по техническим каналам
		Разработка программно-технических средств защиты информации от несанкционированного доступа
		Разработка технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок
		Разработка технических средств контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам
		Разработка программных

Область профессиональной деятельности (по Реестру Минтруда)	Обобщенная трудовая функция	Трудовая функция
		(программно-технических) средств контроля защищенности информации от несанкционированного доступа
	Проектирование объектов в защищенном исполнении	Проектирование средств и систем информатизации в защищенном исполнении
		Проектирование систем защиты информации на объектах информатизации
		Проектирование выделенных (защищаемых) помещений
	Проведение аттестации объектов на соответствие требованиям по защите информации	Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации
		Проведение аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации
	Проведение сертификационных испытаний средств защиты информации на соответствие требованиям по безопасности информации	Проведение сертификационных испытаний на соответствие требованиям безопасности информации технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок
		Проведение сертификационных испытаний на соответствие требованиям безопасности информации технических средств защиты акустической речевой информации от утечки по техническим каналам
		Проведение сертификационных испытаний на соответствие требованиям по безопасности информации программных (программно-технических) средств защиты информации от несанкционированного доступа
		Проведение сертификационных испытаний на соответствие требованиям по безопасности информации технических средств обработки информации в

Область профессиональной деятельности (по Реестру Минтруда)	Обобщенная трудовая функция	Трудовая функция
		защищенном исполнении
		Проведение сертификационных испытаний на соответствие требованиям по безопасности информации технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок
		Проведение сертификационных испытаний на соответствие требованиям по безопасности информации технических средств контроля эффективности мер защиты акустической речевой информации от утечки по техническим каналам
		Проведение сертификационных испытаний на соответствие требованиям по безопасности информации программных (программно-технических) средств контроля защищенности информации от несанкционированного доступа
	Организация и проведение работ по технической защите информации	Создание системы защиты информации в организации
		Ввод в эксплуатацию системы защиты информации в организации
		Сопровождение системы защиты информации в ходе ее эксплуатации

2.3. Перечень основных задач профессиональной деятельности выпускников

Выпускник, освоивший программу магистратуры, готов решать профессиональные задачи, указанные в таблице 2.2.

Таблица 2.2.

Область профессиональной деятельности (по Реестру Минтруда)	Типы/виды задач профессиональной деятельности	Задачи профессиональной деятельности
Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи от несанкционированного доступа к ним (06.030) Автоматизация информационно-аналитической деятельности (АИАД) в государственных органах, обеспечивающих национальную безопасность (06.031) Защита информации в компьютерных системах и сетях (06.032) Обеспечение безопасности информации в автоматизированных системах (06.033) Техническая защита информации (06.034)	Проектная деятельность	Системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности
		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
		Разработка программ и методик испытаний средств и систем обеспечения информационной безопасности
Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи от несанкционированного доступа к ним (06.030) Автоматизация информационно-аналитической деятельности (АИАД) в государственных органах, обеспечивающих национальную безопасность (06.031) Защита информации в компьютерных системах и сетях (06.032) Обеспечение безопасности информации в автоматизированных системах (06.033)	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

Область профессиональной деятельности (по Реестру Минтруда)	Типы/виды задач профессиональной деятельности	Задачи профессиональной деятельности
Техническая защита информации (06.034)		
Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи от несанкционированного доступа к ним (06.030) Автоматизация информационно-аналитической деятельности (АИАД) в государственных органах, обеспечивающих национальную безопасность (06.031) Защита информации в компьютерных системах и сетях (06.032) Обеспечение безопасности информации в автоматизированных системах (06.033) Техническая защита информации (06.034)	Организационно-управленческая деятельность	Организация работы коллектива исполнителей, принятие управленческих решений, определение порядка выполнения работ
		Организация управления информационной безопасностью
		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
		Разработка проектов организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности

3. Планируемые результаты освоения ООП

Результаты освоения ООП ВО определяются приобретаемыми выпускником компетенциями, т.е. его способностью применять знания, умения и личные качества в соответствии с задачами профессиональной деятельности.

Индикаторы достижения компетенций представлены в таблицах 3.1-3.3.

Таблица 3.1. Универсальные компетенции (УК).

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника	Индикаторы достижения универсальной компетенции
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Анализирует проблемную ситуацию как систему, осуществляет ее декомпозицию на отдельные задачи, выявляя ее составляющие и связи между ними.
		УК-1.2. Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению.
		УК-1.3. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников.
		УК-1.4. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов.
		УК-1.5. Строит сценарии реализации стратегии, определяя возможные риски и предлагая пути их устранения, формирует возможные варианты решения задач.
		УК-1.6. Знает методы и средства осуществления саморазвития, как специалиста по информационной безопасности, в условиях неопределенности.
		УК-1.7. Умеет: анализировать условия окружающей действительности и выбирать наиболее оптимальный путь саморазвития, как специалиста по информационной безопасности, в условиях неопределенности; применять методы и средства осуществления

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника	Индикаторы достижения универсальной компетенции
		саморазвития, как специалиста по информационной безопасности, в условиях неопределенности; выявлять недостающие необходимые, как специалисту по информационной безопасности, компетенции и развивать их.
		УК-1.8. Владеет навыками анализа условий окружающей действительности и выбора наиболее оптимального пути саморазвития, как специалиста по информационной безопасности, в условиях неопределенности; владеет навыками применения способов решения возникающих жизненных задач и средств развития (в том числе с использованием цифровых средств) других необходимых, как специалисту по информационной безопасности, компетенций.
		УК-1.9. Знает: методы и способы фильтрации, анализа и оценки информации, ее достоверности; способы и алгоритмы построения логических умозаключений на основе поступающих информации и данных.
		УК-1.10. Умеет: применять методы и способы фильтрации, анализа и оценки информации, ее достоверности; применять способы и алгоритмы построения логических умозаключений на основе поступающих информации и данных.
		УК-1.11. Владеет навыками применения: методов и способов фильтрации, анализа и оценки информации, ее достоверности; способов и алгоритмов построения логических умозаключений на основе поступающих информации и данных.
Разработка и реализация проектов	УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления.
		УК-2.2. Разрабатывает концепцию проекта

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника	Индикаторы достижения универсальной компетенции
		в рамках обозначенной проблемы: формулирует цель, задачи, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения.
		УК-2.3. Разрабатывает план реализации проекта с учетом возможных рисков реализации и возможностей их устранения, планирует необходимые ресурсы.
		УК-2.4. Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта на всех этапах его жизненного цикла.
		УК-2.5. Предлагает процедуры и механизмы оценки качества проекта, инфраструктурные условия для внедрения результатов проекта.
		УК-2.6. Знает: стандартные модели, алгоритмы и методы решения стандартных задач анализа инцидентов информационной безопасности; способы и методики, применяемые для генерации новых идей, поиска нестандартных моделей, новых алгоритмов, способов решения задач анализа инцидентов информационной безопасности.
		УК-2.7. Умеет применять способы и методики, помогающие в генерации новых идей, поиске нестандартных моделей, новых оптимальных алгоритмов, способов решения задач анализа инцидентов информационной безопасности.
		УК-2.8. Владеет навыками: генерации новых идей для решения нестандартных задач анализа инцидентов информационной безопасности, цифровой экономики; абстрагирования от стандартных моделей при решении нестандартных задач анализа инцидентов

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника	Индикаторы достижения универсальной компетенции
		информационной безопасности, цифровой экономики; перестроения сложившихся способов решения нестандартных задач анализа инцидентов информационной безопасности, цифровой экономики; выработки новых оптимальных алгоритмов действий при решении нестандартных задач анализа инцидентов информационной безопасности, цифровой экономики.
		УК-2.9. Знает: современные способы, методы и цифровые средства управления (поиска, анализа, синтеза) информацией и данными при решении задач в областях Big Data и Data Mining; способы и методы критического анализа информации и данных в областях Big Data и Data Mining.
		УК-2.10. Умеет применять современные способы, методы и цифровые средства управления (поиска, анализа, синтеза) информацией и данными при решении задач в областях Big Data и Data Mining; использовать способы и методы критического анализа информации и данных в областях Big Data и Data Mining.
		УК-2.11. Владеет навыками: применения современных способов, методов и цифровых средств управления (поиска, анализа, синтеза) информацией и данными при решении задач в областях Big Data и Data Mining; применения способов и методов критического анализа информации и данных в областях Big Data и Data Mining.
Командная работа и лидерство	УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1. Вырабатывает стратегию командной работы и на ее основе организует отбор членов команды для достижения поставленной цели.
		УК-3.2. Организует и корректирует работу команды, в том числе на основе коллегиальных решений.
		УК-3.3. Разрешает конфликты и

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника	Индикаторы достижения универсальной компетенции
		противоречия при деловом общении на основе учета интересов всех сторон; создает рабочую атмосферу, позитивный эмоциональный климат в команде.
		УК-3.4. Организует обучение членов команды и обсуждение результатов работы, в т.ч. в рамках дискуссии с привлечением оппонентов.
		УК-3.5. Делегирует полномочия членам команды и распределяет поручения, дает обратную связь по результатам, принимает ответственность за общий результат.
Коммуникация	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Устанавливает контакты и организует общение в соответствии с потребностями совместной деятельности, используя современные коммуникационные технологии.
		УК-4.2. Составляет в соответствии с нормами русского языка деловую документацию разных жанров.
		УК-4.3. Составляет типовую деловую документацию для академических и профессиональных целей на иностранном(ых) языке(ах).
		УК-4.4. Создает различные академические или профессиональные тексты на иностранном(ых) языке(ах), а также осуществляет их переводы с иностранного(ых) языка(ов) или на иностранный(ые) язык(и).
		УК-4.5. Организует обсуждение результатов исследовательской и проектной деятельности на различных публичных мероприятиях на русском языке, выбирая наиболее подходящий формат.
		УК-4.6. Представляет результаты исследовательской и проектной деятельности на различных публичных мероприятиях, участвует в академических и профессиональных дискуссиях на

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника	Индикаторы достижения универсальной компетенции
		иностранном(ых) языке(ах).
Межкультурное взаимодействие	УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1. Понимает возможность существования особенностей различных культур и наций.
		УК-5.2. Владеет навыками анализа разнообразия культур и религий.
		УК-5.3. Выстраивает социальное взаимодействие, учитывая общее и особенное различных культур и религий.
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки.	УК-6.1. Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания.
		УК-6.2. Определяет приоритеты личностного роста, образовательные потребности и способы совершенствования собственной (в том числе профессиональной) деятельности на основе самооценки.
		УК-6.3. Выбирает и реализует с использованием инструментов непрерывного образования возможности развития профессиональных компетенций и социальных навыков.
		УК-6.4. Выстраивает гибкую профессиональную траекторию с учетом накопленного опыта профессиональной деятельности, динамично изменяющихся требований рынка труда и стратегии личного развития.
		УК-6.5. Знает методы и средства осуществления саморазвития, как специалиста по информационной безопасности, в условиях неопределенности.
		УК-6.6. Умеет: анализировать условия окружающей действительности и выбирать наиболее оптимальный путь саморазвития, как специалиста по

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника	Индикаторы достижения универсальной компетенции
		информационной безопасности, в условиях неопределенности; применять методы и средства осуществления саморазвития, как специалиста по информационной безопасности, в условиях неопределенности; выявлять недостающие необходимые, как специалисту по информационной безопасности, компетенции и развивать их.
		УК-6.7. Владеет навыками анализа условий окружающей действительности и выбора наиболее оптимального пути саморазвития, как специалиста по информационной безопасности, в условиях неопределенности; владеет навыками применения способов решения возникающих жизненных задач и средств развития (в том числе с использованием цифровых средств) других необходимых, как специалисту по информационной безопасности, компетенций.

Таблица 3.2. Общепрофессиональные компетенции (ОПК).

Категория (группа) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции выпускника	Индикаторы достижения общепрофессиональной компетенции
Теоретическая и практическая профессиональная подготовка	ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на её создание	ОПК-1.1.1. Знает основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности. ОПК-1.2.1. Умеет проектировать информационные системы с учётом различных технологий обеспечения информационной безопасности. ОПК-1.3.1. Владеет навыками участия в разработке системы обеспечения информационной безопасности объекта. ОПК-1.1.2. Знает направления развития и проблемы компьютерного моделирования сложных систем; направления развития технологий проектирования информационных, автоматизированных и автоматических систем. ОПК-1.1.3. Знает современную нормативную базу и ГОСТы, регламентирующие процесс разработки ТЗ; правила, способы и методы организации совместных разработок. ОПК-1.1.4. Знает методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности. ОПК-1.2.2. Умеет обосновывать и планировать состав и архитектуру моделируемых сложных систем; обосновывать и планировать состав и архитектуру проектируемых информационных, автоматизированных и автоматических систем. ОПК-1.2.3. Умеет формировать актуальную модель угроз для АИС и учитывать её положения при формировании требований ТЗ на проектируемую систему обеспечения ИБ. ОПК-1.2.4. Умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения ИБ, оценивать эффективность решений и анализировать показатели деятельности. ОПК-1.2.5. Умеет обосновывать принципы организации технического, программного

Категория (группа) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции выпускника	Индикаторы достижения общепрофессиональной компетенции
		и информационного обеспечения информационной безопасности. ОПК-1.3.2. Владеет навыками разработки концептуальных стратегий решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения ИБ. ОПК-1.3.3. Владеет навыками планирования и оценки трудоёмкости проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений.
	ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.1.1. Знает методы концептуального проектирования технологий обеспечения информационной безопасности. ОПК-2.2.1. Умеет выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью. ОПК-2.3.1. Владеет навыками выполнения работы по изготовлению, монтажу, наладке, испытаниям и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности. ОПК-2.1.2. Знает направления развития и проблемы компьютерного моделирования сложных систем, направления развития технологий проектирования информационных, автоматизированных и автоматических систем. ОПК-2.1.3. Знает современные методы и средства тестирования. ОПК-2.2.2. Умеет разрабатывать тестовые планы и сценарии тестирования разработанного продукта. ОПК-2.2.3. Умеет управлять коллективом исполнителей и принимать управленческие решения. ОПК-2.3.2. Владеет навыками практической реализации типовых задач разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью.

Категория (группа) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции выпускника	Индикаторы достижения общепрофессиональной компетенции
		ОПК-2.3.3. Владеет средствами автоматизированного и ручного функционального тестирования. ОПК-2.1.4. Знает принципы построения и функционирования современных информационных систем. ОПК-2.1.5. Знает назначение комплексной системы защиты информации, принципы её организации и этапы разработки. ОПК-2.1.6. Знает требования к системам комплексной защиты информации. ОПК-2.2.4. Умеет проектировать подсистемы безопасности информационных систем с учётом действующих нормативных и методических документов. ОПК-2.2.5. Умеет разрабатывать модели угроз и нарушителей информационной безопасности информационных систем. ОПК-2.3.4. Владеет навыками участия в организации комплексной системы защиты объекта.
	ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.1.1. Знает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов. ОПК-3.2.1. Умеет разрабатывать технические задания на создание подсистем обеспечения информационной безопасности. ОПК-3.2.2. Умеет проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности. ОПК-3.3.1. Владеет навыками разработки политик безопасности различных уровней. ОПК-3.3.2. Владеет навыками расчёта и управления рисками информационной безопасности, навыками разработки положения о применимости механизмов контроля в контексте управления рисками информационной безопасности.

Категория (группа) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции выпускника	Индикаторы достижения общепрофессиональной компетенции
		ОПК-3.1.2. Знает правила создания технического задания на создание подсистем безопасности информационных систем. ОПК-3.1.3. Знает основные угрозы безопасности информации и модели нарушителя в информационных системах. ОПК-3.2.3. Умеет разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации. ОПК-3.2.4. Умеет разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации. ОПК-3.3.3. Владеет правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации. ОПК-3.1.4. Знает основные нормативные правовые акты в области обеспечения информационной безопасности. ОПК-3.1.5. Знает нормативные методические документы ФСБ России в области защиты информации. ОПК-3.1.6. Знает нормативные методические документы ФСТЭК России в области информационной безопасности. ОПК-3.2.5. Умеет разрабатывать организационно-распорядительную документацию по обеспечению информационной безопасности. ОПК-3.2.6. Умеет работать с технической и эксплуатационной документацией. ОПК-3.2.7. Умеет оценивать различные инструменты в области проектирования и управления информационной безопасностью. ОПК-3.3.4. Владеет навыками работы с нормативными правовыми актами в области информационной безопасности.
Подготовка к исследовательской деятельности	ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать	ОПК-4.1.1. Знает способы формулирования научной проблемы, гипотезы, выбора предмета, объекта, целей, задач исследования. ОПК-4.1.2. Знает основные принципы

Категория (группа) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции выпускника	Индикаторы достижения общепрофессиональной компетенции
	планы и программы проведения научных исследований и технических разработок	создания эскизного, технического, рабочего проектов. ОПК-4.2.1. Умеет составлять пошаговый план научной деятельности, проводить предпроектные исследования. ОПК-4.2.2. Умеет работать с научной литературой, отбирать информацию по теме научного исследования, систематизировать, классифицировать полученную информацию. ОПК-4.3.1. Владеет навыками структурирования информации по теме исследования. ОПК-4.3.2. Владеет навыками самостоятельного научного мышления, обобщения и систематизации информации. ОПК-4.3.3. Владеет навыками сбора и обработки информации в глобальной компьютерной сети, в том числе в мультидисциплинарных реферативных базах данных Scopus, Web of Knowledge. ОПК-4.3.4. Владеет методикой создания технического задания и технического проекта при организации НИОКР. ОПК-4.1.3. Знает методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных систем. ОПК-4.1.4. Знает современные достижения науки в области информационной безопасности. ОПК-4.2.3. Умеет определять комплекс мер для обеспечения безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности систем. ОПК-4.2.4. Умеет использовать методы и средства анализа защищенности информационных систем. ОПК-4.3.5. Владеет программными и программно-аппаратными средствами анализа систем защиты информации. ОПК-4.1.5. Знает правила, способы и методы организации, выполнения и представления результатов научного исследования. ОПК-4.1.6. Знает правила и стандарты

Категория (группа) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции выпускника	Индикаторы достижения общепрофессиональной компетенции
		разработки отчетной документации. ОПК-4.1.7. Знает основные категории и понятия информационно-аналитической работы, принципы и методы ее ведения. ОПК-4.1.8. Знает методы выработки и принятия информационного решения. ОПК-4.2.5. Умеет использовать программные и аппаратные средства персонального компьютера для поиска и обработки информации. ОПК-4.2.6. Умеет разрабатывать планы и программы проведения научных исследований в соответствии с техническим заданием, ресурсным обеспечением и заданными сроками выполнения работы. ОПК-4.3.6. Владеет навыками поиска информации в глобальной информационной сети Интернет. ОПК-4.3.7. Владеет методологией научных исследований в сфере информационной безопасности ОПК-4.1.9. Знает технологии поиска, изучения, обобщения и систематизации научной информации. ОПК-4.1.10. Знает виды отчетно-информационных документов, методы их подготовки. ОПК-4.1.11. Знает основные теоретико-числовые методы применительно к задачам защиты информации. ОПК-4.2.7. Умеет представлять результаты научно-исследовательской деятельности в виде презентаций, отчетов, устных докладов. ОПК-4.2.8. Умеет логически мыслить, вести научные дискуссии. ОПК-4.3.8. Умеет использовать справочную и научную литературу по тематике решаемых информационных задач, оценивать специальную информацию, систематизировать ее, принимать решение о ее дальнейшем использовании. ОПК-4.3.9. Владеет навыками планирования научного исследования. ОПК-4.3.10. Владеет основными методами поиска и структурирования информации.

Категория (группа) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции выпускника	Индикаторы достижения общепрофессиональной компетенции
	ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	ОПК-5.1.1. Знает теоретические и эмпирические методы научных исследований. ОПК-5.1.2. Знает порядок проведения научных исследований. ОПК-5.1.3. Знает методику проведения патентных исследований, объектом которых могут являться объекты техники, промышленной и интеллектуальной собственности (изобретения, полезные модели, программы для ЭВМ и базы данных и др.), ноу-хау и пр. ОПК-5.2.1. Умеет применять методы научных исследований в научной деятельности, в частности, при написании магистерской диссертации и научных статей. ОПК-5.2.2. Умеет составлять отчеты о патентных исследованиях по ГОСТ. ОПК-5.3.1. Владеет навыками оформления научных публикаций в соответствие с шаблоном IEEE, требованиями научных конференций. ОПК-5.3.2. владеет теоретическими и эмпирическими методами научного исследования при выполнении научно-исследовательских работ. ОПК-5.3.3. Владеет методикой оформления отчетов по научно-исследовательским работам согласно ГОСТ. ОПК-5.1.4. Знает порядок организации процесса исследования эффективности системы управления ИБ. ОПК-5.2.3. Умеет формализовать задачи анализа безопасности информационных систем, разрабатывать методики исследования и применять инструментальные средства анализа безопасности. ОПК-5.3.4. Владеет навыками выбора и обоснования критериев оценки защищенности открытых информационных систем. ОПК-5.3.5. Владеет навыками обработки, оценки и представления результатов исследования эффективности решений по управлению информационной

Категория (группа) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции выпускника	Индикаторы достижения общепрофессиональной компетенции
		безопасностью. ОПК-5.1.5. Знает нормативные и методические материалы в сфере информационной безопасности. ОПК-5.1.6. Знает принципы организации технического, программного и информационного обеспечения информационной безопасности. ОПК-5.1.7. Знает методы построения оптимальных планов для научных экспериментов. ОПК-5.2.4. Умеет составлять и корректировать план проведения работ в зависимости от полученных результатов ОПК-5.3.6. Владеет навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации. ОПК-5.1.8. Знает правила, способы и методы организации, выполнения и представления результатов научного исследования. ОПК-5.1.9. Знает принципы построения и функционирования современных информационных систем. ОПК-5.1.10. Знает основные элементы научно-технического эксперимента. ОПК-5.1.11. Знает приемы выбора основных факторов эксперимента и технологию построения факторных планов. ОПК-5.2.5. Умеет оформлять и представлять результаты, полученные в ходе выполнения научно-исследовательского проекта грамотно, лаконично, в достаточном объеме на русском и иностранном языках. ОПК-5.2.6. Умеет выбирать и применять в профессиональной деятельности экспериментальные и расчетно-теоретические методы исследований. ОПК-5.3.7. Владеет навыками анализа получаемых результатов и формулировки выводов. ОПК-5.3.8. Владеет навыками формирования и аргументированного обоснования собственной позиции по

Категория (группа) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции выпускника	Индикаторы достижения общепрофессиональной компетенции
		различным проблемам защиты информации. ОПК-5.1.12. Знает требования ГОСТов на оформление научно-технической документации. ОПК-5.1.13. Знает современные модели и методы измерения, прогнозирования, принятия решений при решении практических задач. ОПК-5.1.14. Знает принципы построения вероятностных моделей применительно к практическим задачам. ОПК-5.2.7. Умеет работать со специальными программными средствами для оформления проектной и отчетной документации. ОПК-5.2.8. Умеет обобщать полученные экспериментальные данные, анализировать и делать выводы. ОПК-5.3.9. Владеет навыками представления результатов работы в виде презентаций, пояснительных записок, научных докладов и статей. ОПК-5.3.10. Владеет навыками самостоятельной работы, самоорганизации.

Таблица 3.3. Профессиональные компетенции (ПК).

Код и наименование профессиональной компетенции выпускника	Индикаторы достижения профессиональной компетенции
ПК-1. Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты.	ПК-1.1. Способен анализировать направления развития информационных (телекоммуникационных) технологий. ПК-1.2. Способен прогнозировать эффективность функционирования объектов защиты. ПК-1.3. Способен оценивать затраты и риски объектов защиты. ПК-1.4. Способен формировать политику безопасности объектов защиты.
ПК-2. Способен разрабатывать системы и комплексы обеспечения информационной безопасности.	ПК-2.1. Знает принципы и особенности проектирования и разработки систем и комплексов обеспечения информационной безопасности. ПК-2.2. Способен разрабатывать системы и комплексы

Код и наименование профессиональной компетенции выпускника	Индикаторы достижения профессиональной компетенции
	обеспечения информационной безопасности. ПК-2.3. Знает: современные способы, методы и цифровые средства управления (поиска, анализа, синтеза) информацией и данными при решении задач в областях Big Data и Data Mining; способы и методы критического анализа информации и данных в областях Big Data и Data Mining. ПК-2.4. Умеет применять современные способы, методы и цифровые средства управления (поиска, анализа, синтеза) информацией и данными при решении задач в областях Big Data и Data Mining; использовать способы и методы критического анализа информации и данных в областях Big Data и Data Mining. ПК2.5. Владеет навыками: применения современных способов, методов и цифровых средств управления (поиска, анализа, синтеза) информацией и данными при решении задач в областях Big Data и Data Mining; применения способов и методов критического анализа информации и данных в областях Big Data и Data Mining.
ПК-3. Способен организовать управление информационной безопасностью.	ПК-3.1. Знает принципы, методы и средства организации управления информационной безопасностью. ПК-3.2. Способен организовать управление информационной безопасностью
ПК-4. Способен организовывать работу по созданию или модернизации систем обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России.	ПК-4.1. Знает положения правовых нормативных актов и нормативных методических документов ФСБ России, ФСТЭК России по созданию или модернизации систем обеспечения информационной безопасности. ПК-4.2. Способен организовывать работу по созданию или модернизации систем обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России.
ПК-5. Способен принимать значимость информационной безопасности, как системообразующего фактора сфер жизни современного общества, ее влияния на состояние экономической, политической, оборонной и других составляющих национальной безопасности.	ПК-5.1. Знает направления и тенденции развития современных вычислительных и информационно-коммуникационных средств и систем, средств обеспечения информационной безопасности. ПК-5.2. Способен определять актуальные угрозы безопасности защищаемого объекта информатизации. ПК-5.3. Способен принимать значимость информационной безопасности, как системообразующего фактора сфер жизни современного общества, ее влияния на состояние экономической, политической, оборонной и других составляющих национальной безопасности.
ПК-6. Способен выявлять, анализировать и устранять	ПК-6.1. Знает источники возникновения различных технических каналов утечки информации, принципы

Код и наименование профессиональной компетенции выпускника	Индикаторы достижения профессиональной компетенции
различные каналы утечки и средства съёма информации, используемые техническими разведками, а также применять методы и средства противодействия техническим разведкам.	функционирования и устройство средств съема информации. ПК-6.2. Способен выявлять, анализировать и устранять различные каналы утечки и средства съема информации, используемые техническими разведками. ПК-6.3. Способен применять методы и средства противодействия техническим разведкам.

4. Документы, регламентирующие структуру, содержание и организацию образовательного процесса при реализации ООП

4.1. Учебный план и календарный учебный график

В календарном учебном графике указывается последовательность реализации ООП по годам, включая теоретическое обучение, практики, промежуточные и государственную итоговую аттестации, каникулы. Календарный учебный график разработан в соответствии с требованиями ФГОС ВО и других нормативно-правовых документов Российской Федерации, а также локальных нормативных актов Университета. Календарный учебный график представлен в составе учебного плана.

В учебном плане отображается структура ООП ВО – программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность (профиль: Управление информационной безопасностью в органах государственной власти).

Таблица 4.1

Структура ООП		**Объем ООП в з.е.**
Блок 1	Дисциплины (модули)	63
Блок 2	Практика	51
Блок 3	Государственная итоговая аттестация	6
Объем программы магистратуры		120

Учебный план включает обязательную часть и часть, формируемую участниками образовательных отношений.

В обязательную часть включены:

- дисциплины (модули) и практики, обеспечивающие формирование общепрофессиональных компетенций, определяемых ФГОС ВО;
- обязательные дисциплины (модули), указанные в пункте 2.2 ФГОС ВО;
- дисциплины (модули) и практики, обеспечивающие формирование универсальных компетенций.

В часть, формируемую участниками образовательных отношений, включены:

- дисциплины (модули) и практики, обеспечивающие формирование профессиональных компетенций;
- дисциплины (модули) и практики, обеспечивающие формирование универсальных компетенций.

Объем обязательной части без учета объема государственной итоговой аттестации – 62 зачетных единицы, что составляет 51,7 процента от общего объема программы магистратуры.

Учебный план регламентирует перечень и последовательность освоения дисциплин (модулей) и практик, формы и сроки прохождения промежуточной аттестации. В учебном плане указывается общий объем дисциплин (модулей), практик в зачетных единицах, а также объем

контактной и самостоятельной работы обучающихся в часах. Для каждой дисциплины (модуля) в учебном плане указываются виды контактной работы.

Максимальный объем учебной нагрузки обучающегося составляет 54 часа в неделю, включая все виды контактной и самостоятельной работы. В указанный объем не входят факультативные дисциплины.

Объем контактной работы обучающихся с педагогическими работниками при проведении учебных занятий по программе магистратуры при очной форме обучения составляет 50,35 % объема программы магистратуры, отводимого на реализацию дисциплин (модулей) (согласно ФГОС ВО – не менее 50%), при очно-заочной форме обучения – 51,94 % (согласно ФГОС – не менее 25 %).

Максимальный объем контактной работы при освоении ООП при очной и очно-заочной формах обучения составляет 16 академических часов в неделю. В указанный объем не входит контактная работа по факультативным дисциплинам. Минимальный объем контактной работы составляет при очной форме обучения – 14 академических часов в неделю, при очно-заочной форме обучения - 12 академических часов в неделю.

Объем факультативных дисциплин составляет 4 зачетных единиц.

Обучающимся обеспечивается возможность освоения дисциплин по выбору, в том числе специализированные условия инвалидам и лицам с ограниченными возможностями здоровья.

Объем каникулярного времени в учебном году определяется настоящей ООП с учетом требований Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденный приказом Минобрнауки России от 6 апреля 2021 г. № 245 и отражается в календарном учебном графике.

4.2. Рабочие программы дисциплин (модулей)

В состав ООП магистратуры входят рабочие программы всех дисциплин (модулей), перечисленных в утвержденном учебном плане.

Рабочие программы дисциплин содержат следующие разделы:

1. Планируемые результаты обучения по дисциплине, ее объем и место в структуре ООП.
2. Содержание и структура дисциплины.
3. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине.
4. Фонды оценочных средств для проведения текущего контроля успеваемости.
5. Фонды оценочных средств для промежуточной аттестации обучающихся по дисциплине.
6. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины.
7. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины.
8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.
9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Рабочие программы дисциплин (модулей) разработаны кафедрами, обеспечивающими реализацию этих дисциплин (модулей), рассмотрены и утверждены на заседании кафедры «Информационная безопасность».

Аннотации к рабочим программам дисциплин (модулей) представлены в **Приложении А**.

4.3. Рабочие программы практик

В Блок 2 «Практика» в соответствии с ФГОС ВО по направлению подготовки 10.04.01 «Информационная безопасность» входят производственные практики, в том числе НИР и преддипломная практика. Производственные практики представляют собой вид учебных занятий, непосредственно ориентированный на профессионально-практическую подготовку обучающихся. Практики закрепляют знания и умения, приобретаемые обучающимися в результате освоения дисциплин, вырабатывают практические навыки и способствуют комплексному формированию универсальных, общепрофессиональных и профессиональных компетенций обучающихся.

Практики проводятся в форме практической подготовки.

Практическая подготовка – форма организации образовательной деятельности при освоении образовательной программы в условиях выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по профилю образовательной программы.

В соответствии с ФГОС ВО по направлению подготовки 10.04.01 «Информационная безопасность» Блок 2 «Практика» основной образовательной программы магистратуры может содержать обязательные, рекомендуемые и дополнительные (устанавливаемые образовательной организацией) типы производственных практик.

В соответствии с утвержденным учебным планом практическая подготовка обучающихся по направлению подготовки 10.04.01 «Информационная безопасность» (профиль: Управление информационной безопасностью в органах государственной власти) включает следующие типы производственных практик:

- эксплуатационная практика;
- научно-исследовательская работа;
- преддипломная практика.

Преддипломная практика проводится для выполнения выпускной квалификационной работы и является обязательной.

Все типы практик являются неотъемлемой частью учебного процесса, его продолжением в условиях работы обучающихся в организациях, деятельность которых соответствует профессиональным компетенциям, осваиваемым в рамках ООП (далее – профильная организация), или в структурных подразделениях Университета, предназначенных для проведения практической подготовки.

Содержание и планируемые результаты практики определяются соответствующей программой практики настоящей ООП.

4.3.1. Рабочие программы производственных практик

Тип производственной практики: эксплуатационная практика. Проводится во 2 семестре при очной и очно-заочной формах обучения.

Объем эксплуатационной практики - 6 зачетных единиц при любой форме обучения (4 недели). Способ проведения практики: стационарная. Форма проведения практики при очной и очно-заочной формах обучения во 2 семестре – концентрированная практика.

Основная цель эксплуатационной практики: углубление и закрепление знаний и компетенций, полученных в процессе теоретического обучения, изучение опыта создания и применения защищенных информационных технологий и систем для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств или организаций, приобретение студентами практических навыков и опыта профессиональной работы в организации, учреждении, на предприятии.

Основными задачами эксплуатационной практики являются:

– закрепление, углубление и развитие знаний, полученных в процессе теоретической подготовки в предшествующий период обучения;

– формирование у обучаемых полного представления о своей профессии;

– выполнение обязанностей на первичных должностях служб защиты информации предприятий, других структурных подразделений, имеющих отношение к информационной безопасности;

– получение практических навыков в выполнении комплекса работ по обеспечению информационной безопасности предприятия;

– получение практических навыков в оформлении нормативных документов, регламентирующих деятельность в сфере информационной безопасности;

– изучение организационно-функциональной структуры базы практики;

– расширение представлений о функциональных возможностях защищенных информационных систем;

– усвоение и закрепление навыков самостоятельной работы и самостоятельного решения поставленных задач;

– сбор материала для последующего его использования при изучении учебных дисциплин;

– изучение и определение состава и видов информационных технологий, применяемых на базе практике;

– изучение основных средств защиты информационных технологий, применяемых на базе практике (техническое, программное, лингвистическое обеспечение и т.п.);

– формирование умения анализировать и оценивать свою собственную профессиональную деятельность;

– описание информационных ресурсов, применяемых на базе практики (базы данных, web-ресурсы, архивы и т.п.).

За период прохождения эксплуатационной практики обучающийся должен закрепить знания по всем изученным ранее дисциплинам, получить навыки их практического применения.

Тип производственной практики: научно-исследовательская работа. Проводится в 1, 2 и 3 семестрах при очной и очно-заочной формах обучения. Общий объем - 18 зачетных единиц (по 6 з.е. в каждом семестре). Способ проведения практики: стационарная. Форма проведения практики при очной и очно-заочной формах обучения – рассредоточенная практика.

Основная цель научно-исследовательской работы: изучение опыта создания и применения защищенных информационных технологий и систем для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств, организаций или корпораций; приобретение навыков практического решения задач защиты информации на рабочем месте; подготовка материалов по теме магистерской диссертации.

Основными задачами научно-исследовательской работы являются:

– определение вида и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов, целей и задач деятельности данного объекта обследования;

– выполнение работ по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации на конкретных объектах информатизации;

– описание вида и формы информации, подверженной угрозам, возможных методов и путей реализации угроз на основе анализа структуры и содержания информационных процессов, целей и задач деятельности заданного объекта обследования в рамках темы магистерской диссертации;

– выполнение работ по оформлению магистерской диссертации и разработке ее презентации.

За период прохождения производственной практики (выполнения научно-исследовательской работы) обучающийся должен закрепить знания по всем изученным ранее дисциплинам, получить навыки их практического применения.

Тип производственной практики: эксплуатационная практика. Проводится в 3 и 4 семестрах при очной и очно-заочной формах обучения.

Общий объем эксплуатационной практики - 12 зачетных единиц при любой форме обучения. Способ проведения практики: стационарная. Форма проведения практики при очной и очно-заочной формах обучения – рассредоточенная практика.

Основная цель эксплуатационной практики: углубление и закрепление знаний и компетенций, полученных в процессе теоретического обучения, изучение опыта создания и применения защищенных информационных технологий и систем для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств или организаций, приобретение студентами практических навыков и опыта профессиональной работы в организации, учреждении, на предприятии.

Основными задачами эксплуатационной практики являются:

– закрепление, углубление и развитие знаний, полученных в процессе теоретической подготовки в предшествующий период обучения;

– формирование у обучаемых полного представления о своей профессии;

– выполнение обязанностей на первичных должностях служб защиты информации предприятий, других структурных подразделений, имеющих отношение к информационной безопасности;

– получение практических навыков в выполнении комплекса работ по обеспечению информационной безопасности предприятия;

– получение практических навыков в оформлении нормативных документов, регламентирующих деятельность в сфере информационной безопасности;

– изучение организационно-функциональной структуры базы практики;

– расширение представлений о функциональных возможностях защищенных информационных систем;

– усвоение и закрепление навыков самостоятельной работы и самостоятельного решения поставленных задач;

– сбор материала для последующего его использования при изучении учебных дисциплин;

– изучение и определение состава и видов информационных технологий, применяемых на базе практике;

– изучение основных средств защиты информационных технологий, применяемых на базе практике (техническое, программное, лингвистическое обеспечение и т.п.);

– формирование умения анализировать и оценивать свою собственную профессиональную деятельность;

– описание информационных ресурсов, применяемых на базе практики (базы данных, web-ресурсы, архивы и т.п.).

За период прохождения эксплуатационной практики обучающийся должен закрепить знания по всем изученным ранее дисциплинам, получить навыки их практического применения.

Тип производственной практики: преддипломная практика. Проводится в 4 семестре при очной форме обучения и в 5 семестре – при очно-заочной форме обучения. Объем при очной и очно-заочной формах обучения – 15 зачетных единиц. Способ проведения практики: стационарная при любой форме обучения. Форма проведения практики – концентрированная практика.

Основная цель преддипломной практики: изучение опыта создания и применения защищенных информационных технологий и систем для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств, организаций или корпораций; приобретение навыков практического решения задач защиты информации на рабочем месте; сбор, обработка (анализ), подготовка материалов для написания и написание выпускной квалификационной работы.

Основными задачами преддипломной практики являются:

−углубление знаний, полученных в ходе обучения, развитие навыков их применения в практической области защиты информации;

−расширение представлений о функциональных возможностях защищенных информационных систем;

−усвоение и закрепление навыков самостоятельной работы и самостоятельного решения поставленных задач;

−сбор материала для последующего его использования при написании выпускной квалификационной работы;

−углубление практических умений и навыков по профессиональной деятельности в рамках направления 10.04.01 «Информационная безопасность»;

−приобретение практических навыков по сбору и анализу информационных материалов;

−формирование умения анализировать и оценивать свою собственную профессиональную деятельность.

За период прохождения преддипломной практики обучающийся должен закрепить знания, полученные в процессе обучения на всех курсах, получить навыки их практического применения.

Все типы практик могут проводиться как в профильных организациях г. Севастополя, Республики Крым и других субъектов Российской Федерации, так и в подразделениях Университета (лабораториях, центрах и др.), обладающих необходимым кадровым и научным потенциалом, а также материально-техническим оснащением.

Общее руководство и контроль над организацией и проведением практики возлагается на кафедру «Информационная безопасность». В случае проведения практики в профильной организации назначается также руководитель практики от профильной организации. Проведение практики в профильных организациях осуществляется на основе договоров с этими организациями. В их число входят: ФГУП «Главный радиочастотный центр», ООО ЦЗИ «Флагман», ООО «Крым Инфо», ООО «Экстрим Безопасность», АО «Удостоверяющий центр», ГКУ «Многофункциональный центр предоставления государственных и муниципальных услуг в городе Севастополе», ГУП С «Севтелеком», Крымское управление Ростехнадзора, ООО «ТРК ЭЛАС», ООО «Севстар ИСПС», ООО «КТК ТЕЛЕКОМ», ГУП РК «Крымэнерго», ООО «Лаборатория кибербезопасности», Центральный банк Российской Федерации, ООО «Международный аэропорт Симферополь», АО «Инфовотч», Управление Федерального казначейства, ФГУП «НПП «Гамма», ЗАО «Интегра-С», ГУ МЧС России, Правительство города Севастополя.

В случае проведения практики в профильной организации, содержание и планируемые результаты практики согласовываются с руководителем практики от профильной организации.

Промежуточная аттестация по итогам практики проводится в форме защиты отчета о прохождении практики. По результатам аттестации выставляется зачет с оценкой (дифференцированный зачет).

4.4. Фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации

Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей ООП (текущий контроль успеваемости и промежуточная аттестация) создаются фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации, которые включают типовые задания, контрольные работы, тесты и иные формы и методы контроля, позволяющие оценить планируемые результаты обучения по каждой дисциплине; описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания; методические материалы, определяющие процедуры оценивания знаний, умений и навыков.

Фонды оценочных средств для каждой дисциплины разрабатываются кафедрами, обеспечивающими реализацию этой дисциплины, рассматриваются и утверждаются кафедрой «Информационная безопасность» в составе рабочей программы дисциплины основной образовательной программы.

Формами промежуточной аттестации обучающихся являются зачеты, зачеты с оценкой (дифференцированные зачеты), экзамены, которые проводятся в конце семестра, защита курсового проекта (курсовой работы), защита отчета о прохождении практики.

4.5. Программа государственной итоговой аттестации

Государственная итоговая аттестация (далее – ГИА), завершающая освоение ООП, является обязательной.

Цель ГИА – определение соответствия результатов освоения обучающимися основной образовательной программы соответствующим требованиям ФГОС ВО.

В ходе проведения ГИА проверяется уровень подготовленности обучающихся к решению профессиональных задач, уровень сформированности у выпускников, освоивших ООП, совокупности компетенций в соответствии с требованиями ФГОС ВО, с учетом профиля (специализации) реализуемой образовательной программы.

ГИА обучающихся по данной образовательной программе включает подготовку к процедуре защиты и защиту выпускной квалификационной работы (далее – ВКР).

Программа ГИА включает:

- требования к выпускным квалификационным работам и порядку их выполнения;
- перечень компетенций, уровень сформированности которых оценивается на ГИА.

Порядок подготовки и защиты ВКР, требования к ВКР определяются локальными нормативными актами Университета, а также методическими указаниями кафедры.

4.6. Фонды оценочных средств государственной итоговой аттестации

Фонды оценочных средств для проведения ГИА включают в себя:

- примерный перечень тем выпускных квалификационных работ;
- описание показателей и критериев оценивания результатов защиты выпускных квалификационных работ, уровня сформированности компетенций;
- описание шкал оценивания;
- методические материалы, определяющие процедуру оценивания результатов освоения образовательной программы.

5. Сведения об условиях реализации ООП

Условия реализации ООП определяются требованиями ФГОС ВО к условиям реализации программы магистратуры по направлению подготовки 10.04.01 «Информационная безопасность».

5.1. Общесистемное обеспечение реализации ООП

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.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам) и к электронной информационно-образовательной среде Университета. Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают возможность доступа обучающегося из любой точки, в

которой имеется доступ к информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), как на территории Университета, так и вне ее.

Электронная информационно-образовательная среда организации обеспечивает:

- доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

- формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы со стороны любых участников образовательного процесса.

В случаях невозможности организации реализации программы магистратуры в очной форме, допускается частичная реализация программы магистратуры с применением электронного обучения, дистанционных образовательных технологий. При этом электронная информационно-образовательная среда Организации дополнительно обеспечивает:

- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения основной образовательной программы;

- проведение всех видов учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучении, дистанционных образовательных технологий;

- взаимодействие между участниками образовательного процесса, в том числе синхронное и/или асинхронное взаимодействия посредством сети "Интернет".

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих. Функционирование электронной информационно-образовательной среды соответствует законодательству Российской Федерации.

5.2. Кадровые условия реализации ООП

Реализация программы магистратуры обеспечивается педагогическими работниками Университета, а также лицами, привлекаемыми Университетом к реализации программы магистратуры на иных условиях.

Квалификация педагогических работников Университета соответствует квалификационным требованиям, указанным в Едином квалификационном справочнике должностей руководителей, специалистов и служащих, разделе "Квалификационные характеристики должностей руководителей и специалистов высшего профессионального и дополнительного профессионального образования", утвержденном приказом Министерства здравоохранения и социального развития Российской Федерации от 11 января 2011 г. № 1н (зарегистрирован Министерством юстиции Российской Федерации 23 марта 2011 г., регистрационный № 20237), и профессиональным стандартам.

Доля педагогических работников Университета, участвующих в реализации программы магистратуры, и лиц, привлекаемых Университетом к реализации программы магистратуры на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), ведущих научную, учебно-методическую и (или) практическую работу, соответствующую профилю преподаваемой дисциплины (модуля), составляет более 80 процентов).

Доля педагогических работников Университета, участвующих в реализации программы магистратуры, и лиц, привлекаемых Университетом к реализации программы магистратуры на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), являющихся руководителями и (или) работниками иных организаций, осуществляющих трудовую деятельность в профессиональной сфере, соответствующей профессиональной деятельности, к которой готовятся выпускники, и имеющих стаж работы в данной профессиональной сфере не менее 3 лет, составляет более 5 процентов.

Доля педагогических работников Университета (исходя из количества замещаемых ставок, приведенного к целочисленным значениям) от общего количества лиц, привлекаемых к реализации программы магистратуры, составляет более 55 процентов).

Доля педагогических работников Университета, участвующих в реализации ООП ВО, и лиц, привлекаемых к образовательной деятельности Университета на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), имеющих ученую степень (в том числе ученую степень, полученную в иностранном государстве и признаваемую в Российской Федерации) и (или) ученое звание (в том числе ученое звание, полученное в иностранном государстве и признаваемое в Российской Федерации), составляет более 60 процентов).

Общее руководство научным содержанием программы магистратуры осуществляется профессором кафедры «Информационная безопасность» Гончаренко Юлией Юрьевной, доктором технических наук, доцентом, осуществляющим самостоятельные научно-исследовательские (творческие) проекты (участвующим в осуществлении таких проектов) по направлению подготовки, имеющим ежегодные публикации по результатам указанной научно-исследовательской (творческой) деятельности в ведущих отечественных рецензируемых научных журналах и изданиях, а также осуществляющим ежегодную апробацию результатов указанной научно-исследовательской (творческой) деятельности на национальных и международных конференциях.

Согласно требованиям ФГОС ВО в реализации программы магистратуры должен принимать участие минимум один педагогический работник Университета, имеющий ученую степень или ученое звание по научной специальности 05.13.19 "Методы и системы защиты информации, информационная безопасность" или по научной специальности, соответствующей направлениям подготовки кадров высшей квалификации по программам подготовки научно-педагогических кадров в адъюнктуре, входящим в укрупненную группу специальностей и направлений подготовки 10.00.00 "Информационная безопасность".

5.3. Материально-техническое и учебно-методическое обеспечение реализации ООП

Институт обеспечен помещениями, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой магистратуры, оснащенными оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей), а также помещением для самостоятельной работы обучающихся, оснащенным компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к ЭИОС Университета.

Перечень материально-технического обеспечения, минимально необходимого для реализации программы магистратуры, включает в себя специально оборудованные помещения для проведения учебных занятий:

- лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенную средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации;
- аудиторию (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну;
- специальную библиотеку (библиотеку литературы ограниченного доступа), предназначенную для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа.

Компьютерные (специализированные) классы и лаборатории оборудованы современной вычислительной техникой из расчета одно рабочее место на каждого обучаемого при проведении занятий в данных классах (лабораториях).

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.

Институт обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения и сертифицированными средствами защиты информации, в том числе отечественного производства, состав которых определяется в рабочих программах дисциплин (модулей) и при необходимости обновляется.

Библиотечный фонд Университета укомплектован печатными изданиями из расчета не менее 0,25 экземпляра каждого из изданий, указанных в рабочих программах дисциплин (модулей), программах практик, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль), проходящих соответствующую практику.

Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей) и при необходимости обновляется.

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

5.4. Применяемые механизмы оценки качества образовательной деятельности и подготовки обучающихся

Внутренняя оценка качества образовательной деятельности и подготовки обучающихся по образовательной программе (далее – внутренняя оценка качества) проводится Университетом с целью обеспечения выполнения требований действующего законодательства в области высшего образования, исключения возможных рисков и угроз при реализации программы и достижения запланированных показателей (индикаторов).

Функционирование системы внутренней оценки качества в Университете регламентируется локальными нормативными актами Университета.