МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
"Национальный исследовательский ядерный университет "МИФИ"

УТВЕРЖДЕНО
первый проректор

Нагорнов О.В.

ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

КОМПЕТЕНТНОСТНАЯ МОДЕЛЬ ВЫПУСКНИКА

Кибербезопасность
образовательная программа

10.04.01 Информационная безопасность
направление подготовки/специальность

Магистратура
уровень образования

Институт интеллектуальных кибернетических систем
институт/факультет/филиал

Зарегистрировано в реестре образовательных программ под номером 1303

2025 г

Оглавление

Раздел 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Нормативные документы

- Федеральный закон от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральный государственный образовательный стандарт по направлению подготовки (специальности) 10.04.01 Информационная безопасность и уровню высшего образования Магистратура, утвержденный приказом Минобрнауки России от 26.11.2020 №1455 (далее – ФГОС ВО);
- Образовательный стандарт НИЯУ МИФИ (ОС НИЯУ МИФИ) по направлению подготовки (специальности) 10.04.01 Информационная безопасность и уровню высшего образования Магистратура, утвержденный Ученым советом университета Протокол №18/03 от 31.05.2018 (далее – ОС НИЯУ МИФИ), актуализирован решением Ученого совета НИЯУ МИФИ (протокол №21/11 от 27.07.2021);
- Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры, утвержденный приказом Минобрнауки России от 06.04.2021 №245 (далее – Порядок организации образовательной деятельности);
- Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры, утвержденный приказом Минобрнауки России от 29 июня 2015 г. № 636;
- Положение о практической подготовке обучающихся, утвержденное приказом Министерства науки и высшего образования РФ и Министерства просвещения РФ от 5 августа 2020 г. N 885/390

1.2. Перечень сокращений

з.е.	–	зачетная единица;
ОПК	–	общепрофессиональная компетенция;
ОС НИЯУ МИФИ	–	образовательный стандарт НИЯУ МИФИ.
ОТФ	–	обобщенная трудовая функция;
ТФ	–	трудовая функция;
ПД	–	профессиональная деятельность;
ПК	–	профессиональная компетенция;
ПС	–	профессиональный стандарт;
УК	–	универсальная компетенция;
УКЕ	–	универсальная естественно-научная компетенция;
УКЦ	–	универсальная цифровая компетенция;
ФГОС ВО	–	федеральный государственный образовательный стандарт высшего образования;

Раздел 2. ОБЩАЯ ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Наименование образовательной программы (направленность, профиль, специализация)

Кибербезопасность

2.2. Назначение и цель образовательной программы

Магистерская программа «Кибербезопасность» соответствует современным требованиям в области защиты информации и цифровых систем. Освоение программы позволяет овладеть современными методами и технологиями обеспечения информационной безопасности, включая защиту данных, сетей, программного обеспечения и критически важных инфраструктур. Учащиеся изучают методы предотвращения кибератак, анализа уязвимостей, разработки защищенных систем, а также управления рисками в области информационной безопасности. Программа готовит специалистов, способных противостоять современным киберугрозам, разрабатывать и внедрять комплексные решения для защиты информационных ресурсов. Цель программы – подготовка высококвалифицированных специалистов в области кибербезопасности, обладающих глубокими знаниями и практическими навыками для проектирования, внедрения и управления системами защиты информации, а также способных проводить исследования в области информационной безопасности и разрабатывать инновационные решения для противодействия киберугрозам. Реализация образовательной программы осуществляется в гибридном формате в сочетании традиционных очных занятий и применением электронного обучения и дистанционных образовательных технологий, посредством использования инновационной онлайн-платформы "Яндекс Практикум".

2.3. Квалификация, присваиваемая выпускникам образовательной программы

Квалификация, присваиваемая выпускникам образовательной программы: Магистр.

2.4. Объем программы

Объем программы: 120 зачетных единиц (далее – з.е.).

2.5. Формы обучения

Формы обучения: очная.

2.6. Срок получения образования

При очной форме обучения 2 года

2.7. Области профессиональной деятельности и сферы профессиональной деятельности, в которых выпускники, освоившие программу, могут осуществлять профессиональную деятельность

06 Связь, информационные и коммуникационные технологии

2.8. Перечень предприятий для прохождения практики и трудоустройства выпускников

- АО "Федеральный центр науки и высоких технологий "Специальное научно-производственное объединение "Элерон"
- Общество с ограниченной ответственностью "КРИПТО-ПРО"
- Другие

Раздел 3. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКОВ

3.1. Общее описание профессиональной деятельности выпускников

Типы задач профессиональной деятельности выпускников (профили подготовки): научно-исследовательский, организационно-управленческий, проектный.

Задачи профессиональной деятельности выпускников:

- проводить исследования в области кибербезопасности, включая анализ новых типов киберугроз, разработку методов защиты от них и создание инновационных решений для обеспечения информационной безопасности;
- разрабатывать и внедрять системы защиты информации, включая проектирование защищенных сетевых архитектур, создание механизмов;
- управлять процессами обеспечения информационной безопасности в организациях, включая разработку политик безопасности, управление рисками и координацию действий по предотвращению инцидентов.

Перечень основных объектов (или областей знания) профессиональной деятельности выпускников:

- информационные системы, сети, программное обеспечение, криптографические протоколы и средства защиты данных;
- киберугрозы, методы и технологии защиты информации, модели анализа рисков и уязвимостей;
- процессы управления информационной безопасностью, нормативно-правовая база, организационные структуры и ресурсы.

3.2. Перечень профессиональных стандартов, соответствующих профессиональной деятельности выпускников, освоивших образовательную программу

№ п/п	Код профессионального стандарта	Наименование профессионального стандарта
06 Связь, информационные и коммуникационные технологии		
1	06.032	Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 01.11.2016 №598н

3.3. Перечень основных задач профессиональной деятельности выпускников

Таблица 3.1

Область профессиональной деятельности (по Реестру Минтруда)	Тип задачи профессиональной деятельности (Профиль)	Задача профессиональной деятельности	Объект профессиональной деятельности (или область знания)
06 Связь, информационные и коммуникационные технологии	проектный	разрабатывать и внедрять системы защиты информации, включая проектирование защищенных сетевых архитектур, создание механизмов	информационные системы, сети, программное обеспечение, криптографические протоколы и средства защиты данных
06 Связь, информационные и коммуникационные технологии	научно-исследовательский	проводить исследования в области кибербезопасности, включая анализ новых типов киберугроз, разработку методов защиты от них и создание инновационных решений для обеспечения информационной безопасности	киберугрозы, методы и технологии защиты информации, модели анализа рисков и уязвимостей
06 Связь, информационные и коммуникационные технологии	организационно-управленческий	управлять процессами обеспечения информационной безопасности в организациях, включая разработку политик безопасности, управление рисками и координацию действий по предотвращению инцидентов	процессы управления информационной безопасностью, нормативно-правовая база, организационные структуры и ресурсы

Раздел 4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4.1. Требования к планируемым результатам освоения образовательной программы, обеспечиваемым дисциплинами (модулями) и практиками обязательной части

4.1.1. Универсальные компетенции выпускников и индикаторы их достижения

Таблица 4.1

Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	З-УК-1 Знать: методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации У-УК-1 Уметь: применять методы системного подхода и критического анализа проблемных ситуаций; разрабатывать стратегию действий, принимать конкретные решения для ее реализации В-УК-1 Владеть: методологией системного и критического анализа проблемных ситуаций; методиками постановки цели, определения способов ее достижения, разработки стратегий действий
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	З-УК-2 Знать: этапы жизненного цикла проекта; этапы разработки и реализации проекта; методы разработки и управления проектами У-УК-2 Уметь: разрабатывать проект с учетом анализа альтернативных вариантов его реализации, определять целевые этапы, основные направления работ; объяснить цели и сформулировать задачи, связанные с подготовкой и реализацией проекта; управлять проектом на всех этапах его жизненного цикла В-УК-2 Владеть: методиками разработки и управления проектом; методами оценки потребности в ресурсах и эффективности проекта
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	З-УК-3 Знать: методики формирования команд; методы эффективного руководства коллективами; основные теории лидерства и стили руководства У-УК-3 Уметь: разрабатывать план групповых и организационных коммуникаций при подготовке и выполнении проекта; сформулировать задачи членам команды для достижения поставленной цели; разрабатывать командную стратегию; применять эффективные стили руководства командой для достижения поставленной цели В-УК-3 Владеть: умением анализировать, проектировать и организовывать межличностные, групповые и организационные коммуникации в команде для достижения поставленной цели;

	методами организации и управления коллективом
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	З-УК-4 Знать: правила и закономерности личной и деловой устной и письменной коммуникации; современные коммуникативные технологии на русском и иностранном языках; существующие профессиональные сообщества для профессионального взаимодействия У-УК-4 Уметь: применять на практике коммуникативные технологии, методы и способы делового общения для академического и профессионального взаимодействия В-УК-4 Владеть: методикой межличностного делового общения на русском и иностранном языках, с применением профессиональных языковых форм, средств и современных коммуникативных технологий
УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	З-УК-5 Знать: закономерности и особенности социально-исторического развития различных культур; особенности межкультурного разнообразия общества; правила и технологии эффективного межкультурного взаимодействия У-УК-5 Уметь: понимать и толерантно воспринимать межкультурное разнообразие общества; анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия В-УК-5 Владеть: методами и навыками эффективного межкультурного взаимодействия
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	З-УК-6 Знать: методики самооценки, самоконтроля и саморазвития с использованием подходов здоровьесбережения У-УК-6 Уметь: решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности; применять методики самооценки и самоконтроля; применять методики, позволяющие улучшить и сохранить здоровье в процессе жизнедеятельности В-УК-6 Владеть: технологиями и навыками управления своей познавательной деятельностью и ее совершенствования на основе самооценки, самоконтроля и принципов самообразования в течение всей жизни, в том числе с использованием здоровьесберегающих подходов и методик
УКЦ-1 Способен решать исследовательские, научно-технические и производственные задачи в условиях неопределенности, в том числе выстраивать деловую коммуникацию и организовывать работу команды с использованием цифровых ресурсов и	З-УКЦ-1 Знать современные цифровые технологии, используемые для выстраивания деловой коммуникации и организации индивидуальной и командной работы У-УКЦ-1 Уметь подбирать наиболее релевантные цифровые решения для достижения

технологий в цифровой среде	поставленных целей и задач, в том числе в условиях неопределенности В-УКЦ-1 Владеть навыками решения исследовательских, научно-технических и производственных задач с использованием цифровых технологий
УКЦ-2 Способен к самообучению, самоактуализации и саморазвитию с использованием различных цифровых технологий в условиях их непрерывного совершенствования	З-УКЦ-2 Знать основные цифровые платформы, технологи и интернет ресурсы используемые при онлайн обучении У-УКЦ-2 Уметь использовать различные цифровые технологии для организации обучения В-УКЦ-2 Владеть навыками самообучения, самооактулизации и саморазвития с использованием различных цифровых технологий

4.1.2. Общепрофессиональные компетенции выпускников и индикаторы их достижения

Таблица 4.2

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	З-ОПК-1 Знать: основы стандартов в области обеспечения информационной безопасности; элементы компьютерного моделирования сложных систем, проектирования информационных, автоматизированных и автоматических систем У-ОПК-1 Уметь: проектировать информационные системы; обосновывать и планировать состав и архитектуру моделируемых и проектируемых информационных, автоматизированных и автоматических систем; разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности. В-ОПК-1 Владеть: навыками участия в разработке системы обеспечения информационной безопасности объекта; навыками проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	З-ОПК-2 Знать: методы проектирования технологий обеспечения информационной безопасности; принципы построения и функционирования современных информационных систем; требования к системам комплексной защиты информации У-ОПК-2 Уметь: обосновывать применяемые методы решения задач защиты информации, проектировать подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов, разрабатывать модели угроз и нарушителей

	информационной безопасности В-ОПК-2 Владеть: навыками проектирования систем информационной безопасности
ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	З-ОПК-3 Знать: основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью У-ОПК-3 Уметь: проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации В-ОПК-3 Владеть: навыками разработки политик безопасности различных уровней и работы с нормативными правовыми актами в области информационной безопасности
ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	З-ОПК-4 Знать: способы формулирования научной проблемы, гипотезы, выбора предмета, объекта, целей, задач исследования; методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных систем У-ОПК-4 Уметь: разрабатывать планы и программы проведения научных исследований в соответствии с техническим заданием, ресурсным обеспечением и заданными сроками выполнения работы В-ОПК-4 Владеть: навыками структурирования информации по теме исследования и самостоятельного научного мышления, обобщения и систематизации информации
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	З-ОПК-5 Знать: теоретические и эмпирические методы научных исследований, порядок проведения научных исследований У-ОПК-5 Уметь: применять методы научных исследований в научной деятельности, обобщать полученные экспериментальные данные, анализировать и делать выводы В-ОПК-5 Владеть: теоретическими и эмпирическими методами научного исследования при выполнении научно-исследовательских работ, методикой оформления отчетов по научно-исследовательским работам, статей и тезисов докладов

4.1.3. Обязательные профессиональные компетенции выпускников и индикаторы их достижения

Таблица 4.3

Задача ПД	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС, анализ опыта)	Код и наименование ОТФ (ТФ)
1	2	3	4	5	6
Тип задачи профессиональной деятельности: научно-исследовательский					
проводить исследования в области кибербезопасности, включая анализ новых типов киберугроз, разработку методов защиты от них и создание инновационных решений для обеспечения информационной безопасности	киберугрозы, методы и технологии защиты информации, модели анализа рисков и уязвимостей	ПК-3 Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта	З-ПК-3 Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты сссэ от нсд, зткс; национальные, межгосударственные и международные	Профессиональный стандарт «06.032. Специалист по безопасности компьютерных систем и сетей»	D/02.8. Проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей

			стандарты, устанавливающие требования по защите информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. У-ПК-3 Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности сетей электросвязи. В-ПК-3 Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.		
Тип задачи профессиональной деятельности: организационно-управленческий					
управлять процессами обеспечения информационно	процессы управления информационной безопасностью,	ПК-7 Способен планировать и организовывать предпроектное	З-ПК-7 Знать: основные методы организационного обеспечения	Профессиональный стандарт «06.032. Специалист по безопасности	С/03.7. Проведение анализа безопасности

й безопасности в организациях, включая разработку политик безопасности, управление рисками и координацию действий по предотвращению инцидентов	нормативно-правовая база, организационные структуры и ресурсы	исследование объектов обеспечения ИБ или объектов информационно-аналитических систем безопасности	информационной безопасности иас; основные виды угроз безопасности операционных систем; защитные механизмы и средства обеспечения безопасности операционных систем. У-ПК-7 Уметь: организовывать реализацию мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; определять методы управления доступом, типы доступа и правила разграничения доступа; определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; организовывать процесс применения защищенных протоколов, межсетевых экранов, средств обнаружения вторжений для защиты информации в сетях.	компьютерных систем и сетей»	компьютерных систем

			В-ПК-7 Владеть: основами формирования комплекса мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в иас информации ограниченного доступа.		
		ПК-8 Способен использовать навыки составления и оформления организационно-нормативных документов, научных отчетов, обзоров, докладов и статей в области ИБ или в области информационно-аналитических систем безопасности	З-ПК-8 Знать: профессиональная и криптографическая терминология в области безопасности информации; эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; принципы	Профессиональный стандарт «06.032. Специалист по безопасности компьютерных систем и сетей»	С/03.7. Проведение анализа безопасности компьютерных систем

			организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения. организационно-распорядительная документация по защите информации на объекте информатизации; современные информационные технологии (операционные системы, базы данных, вычислительные сети); технические каналы утечки акустической речевой информации; методы защиты информации от утечки по техническим каналам; способы защиты акустической речевой информации от утечки по техническим каналам. У-ПК-8 Уметь: анализировать программные, архитектурно-технические и схемотехнические		

			решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; проводить комплексное тестирование аппаратных и программных средств; определять перечень информации (сведений)ограниченного доступа, подлежащих защите в организации; определять условия расположения объектов информатизации относительно границ контролируемой зоны; разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации; разрабатывать разрешительную систему доступа к		

			информационным ресурсам, программным и техническим средствам автоматизированных (информационных) систем организации. В-ПК-8 Владеть: основами применения средств схемотехнического проектирования и современной измерительной аппаратуры; основами оптимизации работ электронных схем с учетом требований по защите информации; основами организации проведения научных исследований по вопросам технической защиты информации, выполняемых в организации.		
Тип задачи профессиональной деятельности: проектный					
разрабатывать и внедрять системы защиты информации, включая проектирование защищенных сетевых	информационные системы, сети, программное обеспечение, криптографические протоколы и средства защиты данных	ПК-1 Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности	З-ПК-1 Знать: модели угроз нсд к сетям электросвязи; методики оценки уязвимостей сетей электросвязи с точки зрения возможности нсд к ним; нормативные правовые	Профессиональный стандарт «06.032. Специалист по безопасности компьютерных систем и сетей»	D/02.8. Проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей

архитектур, создание механизмов			акты в области связи, информатизации и защиты информации; виды политик безопасности компьютерных систем и сетей; возможности используемых и планируемых к использованию средств защиты информации; особенности защиты информации в автоматизированных системах управления технологическими процессами; критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; основные характеристики технических средств защиты информации от утечек по техническим каналам; нормативные правовые акты, методические документы, национальные стандарты в области защиты		

			информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации. У-ПК-1 Уметь: выявлять и оценивать угрозы нсд к сетям электросвязи; анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; проводить анализ угроз безопасности информации на объекте информатизации;		

			проводить предпроектное обследование объекта информатизации. В-ПК-1 Владеть: основами проведения технических работ при аттестации сссэ с учетом требований по защите информации; определением угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; основами разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах; основами предпроектного обследования объекта информатизации; основами разработки аналитического обоснования необходимости создания системы защиты информации на объекте		

			информатизации (модели угроз безопасности информации).		
		ПК-2 Способен разрабатывать технические задания на проектирование систем обеспечения ИБ или информационно-аналитических систем безопасности	З-ПК-2 Знать: формальные модели безопасности компьютерных систем и сетей; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; основные угрозы безопасности информации и модели нарушителя; в автоматизированных системах основные меры по защите информации; в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации; в автоматизированных системах; технические средства контроля эффективности мер защиты информации; современные информационные технологии	Профессиональный стандарт «06.032. Специалист по безопасности компьютерных систем и сетей»	D/02.8. Проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей

			(операционные системы, базы данных, вычислительные сети); методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий; средства контроля защищенности информации от несанкционированного доступа. У-ПК-2 Уметь: применять инструментальные средства проведения мониторинга защищенности компьютерных систем; анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации, основные узлы и устройства современных автоматизированных систем; разрабатывать программы и методики испытаний программно-технического средства		

			защиты информации от несанкционированного доступа и специальных воздействий на нее; проводить испытания программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее. В-ПК-2 Владеть: основами выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; основами составлением методик тестирования систем защиты информации автоматизированных систем; основами подбора инструментальных средств тестирования систем защиты информации автоматизированных систем; основами разработки технического задания на создание программно-технического средства		

			защиты информации от несанкционированного доступа и специальных воздействий на нее; основами разработки программ и методик испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами испытаний программно-технического средств защиты информации от несанкционированного доступа и специальных воздействий на нее.		

4.1.4. Профессиональные компетенции выпускников (направленности/профиля/специализации) и индикаторы их достижения

Таблица 4.4

Задача ПД	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС, анализ опыта)	Код и наименование ОТФ (ТФ)
1	2	3	4	5	6
Тип задачи профессиональной деятельности: научно-исследовательский					
проводить исследования в области кибербезопасно	киберугрозы, методы и технологии защиты информации, модели	ПК-11.2 способен разрабатывать и адаптировать методы защиты информации для	З-ПК-11.2 знать современные подходы к анализу и прогнозированию	Профессиональный стандарт «06.032. Специалист по безопасности	D/02.8. Проектирование программно-аппаратных

сти, включая анализ новых типов киберугроз, разработку методов защиты от них и создание инновационных решений для обеспечения информационной безопасности	анализа рисков и уязвимостей	новых типов угроз	киберугроз У-ПК-11.2 уметь проводить исследования в области криптографии, сетевой безопасности и защиты данных В-ПК-11.2 владеть методами моделирования и анализа кибератак	компьютерных систем и сетей»	средств защиты информации компьютерных систем и сетей
Тип задачи профессиональной деятельности: организационно-управленческий					
управлять процессами обеспечения информационной безопасности в организациях, включая разработку политик безопасности, управление рисками и координацию действий по предотвращению инцидентов	процессы управления информационной безопасностью, нормативно-правовая база, организационные структуры и ресурсы	ПК-11.3 способен разрабатывать и внедрять политики и стандарты информационной безопасности	З-ПК-11.3 знать методы управления рисками и инцидентами в области кибербезопасности У-ПК-11.3 уметь координировать действия по защите информации на уровне организации В-ПК-11.3 владеть инструментами для мониторинга и анализа безопасности информационных систем	Профессиональный стандарт «06.032. Специалист по безопасности компьютерных систем и сетей»	С/02.7. Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей
Тип задачи профессиональной деятельности: проектный					
разрабатывать и внедрять	информационные системы, сети,	ПК-11.1 способен проектировать и	З-ПК-11.1 знать современные методы и	Профессиональный стандарт «06.032.	D/02.8. Проектирование

системы защиты информации, включая проектирование защищенных сетевых архитектур, создание механизмов	программное обеспечение, криптографические протоколы и средства защиты данных	внедрять системы защиты информации	технологии кибербезопасности У-ПК-11.1 уметь выявлять и устранять уязвимости в информационных системах В-ПК-11.1 владеть инструментами для тестирования на проникновение и анализа защищенности систем	Специалист по безопасности компьютерных систем и сетей»	программно-аппаратных средств защиты информации компьютерных систем и сетей

Раздел 5. ОРГАНИЗАЦИИ-РАБОТОДАТЕЛИ/ЗАКАЗЧИКИ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

5.1 Перечень организаций-работодателей/заказчиков образовательной программы

– ООО "Яндекс"

Руководитель программы
доцент кафедры 42 _____ / Журин С.И.

Представитель организации-работодателя/заказчика образовательной программы:
ООО "Яндекс"
руководитель образовательных сервисов _____ / Залесский И.И.