МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования

«Московский политехнический университет»

УТВЕРЖДАЮ
Директор департамента
по образовательной политике
_____ /А.Б. Максимов/
«__15__»___февраля___ 2024 г.

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

направление подготовки

10.04.01 Информационная безопасность

направленность (профиль)

«Инженерия безопасности компьютерных систем и сетей»

Уровень образования – магистратура

Квалификация – магистр

Форма обучения – очная

Год начала обучения – 2024 г.

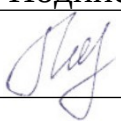
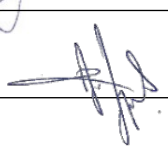
Москва 2024

Лист согласования

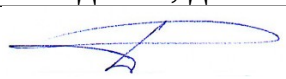
Согласовано:

ФИО	Должность / место работы	Подпись, дата
Демидов Дмитрий Григорьевич	Декан факультета информационных технологий	
Калуцкий Игорь Владимирович	Зав. кафедрой «Информационная безопасность»	

Разработчики:

ФИО	Должность / место работы	Подпись, дата
Гневшев Александр Юрьевич	Ст. преподаватель кафедры «Информационная безопасность»	
Бутакова Наталья Георгиевна	Доцент, к.т.н. кафедры «Информационная безопасность»	

Эксперты:

ФИО	Должность / место работы	Подпись, дата
Лось Владимир Павлович	Президент Ассоциации защиты информации	
Михальский Олег Олегович	Директор по развитию ООО «SiteSecure»	

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящей образовательной программе используются следующие сокращения:

ВО	–	высшее образование;
ОПОП	–	основная профессиональная образовательная программа;
з.е.	–	зачетная единица;
УК	–	универсальная компетенция;
ОПК	–	общепрофессиональная компетенция;
ПК	–	профессиональная компетенция;
ИУК	–	индикатор достижения универсальной компетенции;
ИОПК	–	индикатор достижения общепрофессиональной компетенции;
ИПК	–	индикатор достижения профессиональной компетенции
ОТФ	–	обобщенная трудовая функция;
ОПД	–	область профессиональной деятельности;
ПС	–	профессиональный стандарт;
РПД	–	рабочая программа дисциплины;
ФОС	–	фонд оценочных средств;
ЭИОС	–	электронная информационно-образовательная среда;
ФГОС ВО	–	федеральный государственный образовательный стандарт высшего образования;
ГИА	–	государственная итоговая аттестация;
БИЦ	–	библиотечно-информационный центр;
ЭБС	–	электронно-библиотечная система;
Университет	–	федеральное государственное автономное образовательное учреждение высшего образования «Московский политехнический университет».

I. Нормативное обеспечение реализации образовательной программы

Основой при разработке образовательной программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» являются:

1. Федеральный государственный образовательный стандарт высшего образования (уровень магистратуры) по направлению подготовки 10.04.01 Информационная безопасность, утвержденный приказом Министерства науки и высшего образования РФ от 26 ноября 2020 г. № 1455.
2. Профессиональные стандарты:

– 06.014 Профессиональный стандарт «Менеджер по информационным технологиям». Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 30.08.2021 № 588н;

– 06.032 Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей». Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 533н;

– 06.033 Профессиональный стандарт «Специалист по защите информации в автоматизированных системах». Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н.

II. Общие положения

Цель образовательной программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» состоит в формировании и развитии у обучающихся личностных и профессиональных качеств, позволяющих обеспечить выполнение требований ФГОС ВО с учетом особенностей научно-образовательной школы Университета и актуальных потребностей рынка труда в кадрах с высшим образованием в соответствии с направлением подготовки.

При разработке программы магистратуры сформированы требования к результатам ее освоения в виде универсальных, общепрофессиональных и профессиональных компетенций выпускников.

Обучение по программе магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» осуществляется **в очной форме**.

При реализации программы магистратуры Университет применяет электронное обучение, дистанционные образовательные технологии. Все

материалы размещаются на платформе СДО Московского Политеха (https://online.mospolytech.ru/).

Применение электронного обучения, дистанционных образовательных технологий обеспечивает формирование у обучающихся цифровых компетенций.

Электронное обучение, дистанционные образовательные технологии, применяемые при обучении инвалидов и лиц с ограниченными возможностями здоровья (далее - инвалиды и лица с ОВЗ), предусматривают возможность приема-передачи информации в доступных для них формах.

Реализация программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» осуществляется **посредством сетевой формы** совместно Московским политехническим университетом (базовая организация) и Университетом Иннополис (организация-участник).

Образовательная деятельность по программе магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» осуществляется на государственном языке Российской Федерации – **русском языке**.

Срок получения образования по программе магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» (вне зависимости от применяемых образовательных технологий) в очной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 2 года.

При обучении по индивидуальному учебному плану инвалидов и лиц с ОВЗ срок получения образования может быть увеличен по их заявлению не более чем на полгода.

Объем образовательной программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» составляет 120 з.е. вне зависимости от формы обучения, применяемых образовательных технологий, реализации программы магистратуры с использованием сетевой формы, реализации программы магистратуры по индивидуальному учебному плану.

Объем программы магистратуры, реализуемый за один учебный год, составляет не более 70 з.е. вне зависимости от формы обучения, применяемых образовательных технологий, реализации программы магистратуры с использованием сетевой формы, реализации программы магистратуры по индивидуальному учебному плану (за исключением ускоренного обучения), а при ускоренном обучении – не более 80 з.е.

III. Области, объекты и типы задач профессиональной деятельности выпускника

Области профессиональной деятельности и сферы профессиональной деятельности, в которых выпускники, освоившие программу магистратуры по направлению подготовки 10.04.01 Информационная безопасность, могут осуществлять профессиональную деятельность:

01 Образование и наука (в сфере научных исследований, связанных с обеспечением информационной безопасности и защиты информации);

06 Связь, информационные и коммуникационные технологии (в сфере защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи);

12 Обеспечение безопасности (в сферах: обнаружения, предупреждения и ликвидации последствий компьютерных атак; эксплуатации технических и программно-аппаратных средств защиты информации).

Выпускники могут осуществлять профессиональную деятельность в других областях профессиональной деятельности и (или) сферах профессиональной деятельности при условии соответствия уровня их образования и полученных компетенций требованиям к квалификации работника.

Программа магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» ориентирована на следующие области профессиональной деятельности (ОПД):

06 Связь, информационные и коммуникационные технологии (в сфере защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи).

В рамках освоения программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» выпускники готовятся к решению задач профессиональной деятельности следующих типов:

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

Область профессиональной деятельности выпускников, освоивших программу магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей», включает сферы науки, техники и технологий,

охватывающие совокупность проблем, связанных с обеспечением информационной безопасности и защиты информации.

Объектами профессиональной деятельности выпускников, освоивших программу магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей», 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.

Программа магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» не содержит сведений, составляющих государственную тайну.

IV. Соотнесение профессиональных стандартов с ФГОС ВО

Перечень обобщённых трудовых функций и трудовых функций, соответствующих профессиональной деятельности выпускника программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» представлен в таблице 1.

Таблица 1 – Перечень обобщённых трудовых функций и трудовых функций, соответствующих профессиональной деятельности выпускника программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей»

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
06.014 Менеджер по информационным технологиям	C	Управление единой информационной средой организации, региона, страны	7	Управление рисками ИТ и кибербезопасностью	C/06.7	7
06.032 Специалист по безопасности компьютерных систем и сетей	C	Оценивание уровня безопасности компьютерных систем и сетей	7	Проведение анализа безопасности компьютерных систем	C/03.7	7
				Проведение инструментального мониторинга защищенности компьютерных систем и сетей	C/05.7	
06.033 Специалист по защите информации в автоматизированных системах	C	Разработка систем защиты информации автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости	7	Разработка проектных решений по защите информации в автоматизированных системах	C/02.7	7
				Тестирование систем защиты информации автоматизированных систем	C/01.7	

V. Структура и объем образовательной программы

Структура программы магистратуры включает следующие блоки:

Блок 1 «Дисциплины (модули)».

Блок 2 «Практика».

Блок 3 «Государственная итоговая аттестация».

Таблица 2 – Структура программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей»

Структура программы магистратуры		Объем программы магистратуры и её блоков в з.е.
Блок 1	Дисциплины (модули)	72
Блок 2	Практика	39
Блок 3	Государственная итоговая аттестация	9
Объем программы магистратуры		120

В Блок 2 «Практика» входит производственная практика.

Типы производственной практики:

- научно-исследовательская работа;
- проектно-технологическая;
- преддипломная практика.

В Блок 3 «Государственная итоговая аттестация» входят:

- подготовка к процедуре защиты и защита выпускной квалификационной работы.

Программа магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» обеспечивает обучающимся возможность освоения элективных дисциплин (модулей) и факультативных дисциплин (модулей). Факультативные дисциплины (модули) не включаются в объем программы магистратуры.

Университет предоставляет инвалидам и лицам с ОВЗ (по их заявлению) возможность обучения по программе магистратуры, учитывающей особенности их психофизического развития, индивидуальных возможностей и при необходимости обеспечивающей коррекцию нарушений развития и социальную адаптацию указанных лиц.

Объем контактной работы обучающихся с педагогическими работниками при проведении учебных занятий по программе магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» в очной форме обучения составляет не менее 50 процентов.

VI. Планируемые результаты освоения образовательной программы

В результате освоения программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» у выпускника должны быть сформированы следующие компетенции, установленные программой магистратуры (таблицы 3-5).

Таблица 3 - Универсальные компетенции выпускников и индикаторы их достижения

Категория компетенций	Код и наименование компетенции	Код и содержание индикатора достижения компетенции
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК-1.1. Анализирует проблемную ситуацию как систему, осуществляет её декомпозицию и определяет связи между ее составляющими. ИУК-1.2. Определяет противоречивость и пробелы в информации, необходимой для решения проблемной ситуации, а также критически оценивает релевантность используемых информационных источников. ИУК-1.3. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов с учетом оценки существующих рисков и возможностей их минимизации.
Разработка и реализация проектов	УК-2. Способен управлять проектом на всех этапах его жизненного цикла	ИУК-2.1. Разрабатывает концепцию управления проектом на всех этапах его жизненного цикла в рамках обозначенной проблемы: формулирует цель и пути достижения, задачи и способы их решения, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения. ИУК-2.2. Разрабатывает план реализации проекта в соответствии с существующими условиями, необходимыми ресурсами, возможными рисками и распределением зон ответственности участников проекта.

		ИУК-2.3. Осуществляет мониторинг реализации проекта на всех этапах его жизненного цикла, вносит необходимые изменения в план реализации проекта с учетом количественных и качественных параметров достигнутых промежуточных результатов.
Командная работа и лидерство	УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	ИУК-3.1. Демонстрирует управленческую компетентность, необходимую для формирования команды и руководства ее работой на основе разработанной стратегии сотрудничества. ИУК-3.2. Планирует, организует, мотивирует, оценивает и корректирует совместную деятельность по достижению поставленной цели с учетом интересов, особенностей поведения и мнений ее членов. ИУК-3.3. Применяет способы, методы и стратегии оптимизации социально-психологического климата в коллективе, предупреждения и разрешения конфликтов, технологии обучения и развития профессиональной и коммуникативной компетентности членов команды.
Коммуникация	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	ИУК-4.1. Устанавливает и развивает профессиональные контакты, осуществляет академическое и профессиональное взаимодействие с применением современных коммуникативных технологий, в том числе на иностранном языке. ИУК-4.2. Составляет и редактирует документацию с целью обеспечения академического и профессионального взаимодействия, в том числе на иностранном языке. ИУК-4.3. Демонстрирует коммуникативную компетентность в условиях научно-исследовательской и проектной деятельности и презентации ее результатов на различных публичных мероприятиях, включая международные, в том числе на иностранном языке.
Межкультурное взаимодействие	УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	ИУК-5.1. Анализирует важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития, и обосновывает актуальность их использования при социальном и профессиональном взаимодействии.

		ИУК-5.2. Выстраивает социальное и профессиональное взаимодействие с учетом общих и специфических черт различных культур и религий, особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других наций и конфессий, различных социальных групп. ИУК-5.3. Обеспечивает создание недискриминационной среды взаимодействия при выполнении профессиональных задач, демонстрируя понимание особенностей различных культур и наций.
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	ИУК-6.1. Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания. ИУК-6.2. Определяет приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям. ИУК-6.3. Выстраивает собственную профессиональную траекторию, используя инструменты непрерывного образования, с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда.

Таблица 4 - Общепрофессиональные компетенции выпускников и индикаторы их достижения

Категория компетенций	Код и наименование компетенции	Индикаторы достижения компетенции
	ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИОПК-1.1. Умеет: обосновывать требования к системе обеспечения информационной безопасности; разрабатывать проект технического задания на ее создание.
	ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента	ИОПК-2.1. Умеет: разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.

	системы) обеспечения информационной безопасности	
	ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ИОПК-3.1 Умеет: разрабатывать проекты организационно-распорядительных документов по обеспечению 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	ИОПК-4.1. Умеет: осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок
	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	ИОПК-5.1. Умеет: проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.

Таблица 5 - Профессиональные компетенции выпускников и индикаторы их достижения

ОПД	Основание (ПС, анализ рынка труда, обобщение опыта, проведения консультаций с работодателями)	Код и наименование ОТФ	Коды и наименования трудовых функций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Тип задач профессиональной деятельности: *организационно-управленческий*					
06 Связь, информационные и коммуникационные технологии (в сфере защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи)	06.014 Менеджер по информационным технологиям	C Управление единой информационной средой организации, региона, страны	C/06.7 Управление рисками ИТ и кибербезопасностью	ПК-1. Способен управлять рисками ИТ и кибербезопасностью	**ИПК 1.1. Знает:** - Международные и отечественные стандарты, лучшие практики и фреймворки по управлению рисками ИТ и кибербезопасностью; - Критерии оценки рисков и уровня кибербезопасности; - Методы контроля рисков и уровня кибербезопасности **ИПК 1.2. Умеет:** - Формировать цели и принципы управления рисками ИТ и кибербезопасностью; - Использовать методы и средства обеспечения управления рисками ИТ и кибербезопасностью,

					соответствующие критериям оценки организации; - Формировать команду и организовывать персонал и стейкхолдеров для управления рисками ИТ и кибербезопасностью; - Осуществлять мониторинг и контроль рисков ИТ и кибербезопасности; - Организовывать деятельность по непрерывному улучшению управления рисками ИТ и кибербезопасностью **ИПК 1.3. Владеет:** - навыками применения методов управления рисками для снижения потенциальных угроз и обеспечения безопасности информационных технологий
Тип задач профессиональной деятельности: *научно-исследовательский*					
06 Связь, информационные и коммуникационные технологии (в сфере защиты информации в	06.032 Специалист по безопасности компьютерных систем и сетей	С Оценивание уровня безопасности компьютерных систем и сетей	С/03.7 Проведение анализа безопасности компьютерных систем	ПК-2. Способен проводить анализ безопасности компьютерных систем	**ИПК 2.1 Знает:** - Принципы построения компьютерных систем и сетей; - Уязвимости компьютерных систем и

компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи)					сетей; - Криптографические методы защиты информации; - Принципы построения систем управления базами данных; - Средства анализа конфигураций; - Национальные, межгосударственные и международные стандарты в области защиты информации; - Нормативные правовые акты в области защиты информации; - Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры; - Организационные меры по защите информации. **ИПК 2.2 Умеет:** - Анализировать компьютерную систему с

					целью определения уровня защищенности и доверия; - Прогнозировать возможные пути развития действий нарушителя информационной безопасности; - Производить анализ политики безопасности на предмет адекватности; - Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; - Составлять и оформлять аналитический отчет по результатам проведенного анализа; - Разрабатывать предложения по устранению выявленных уязвимостей **ИПК.2.3 Владеет:** - Навыками выбора режимов работы программно-аппаратных средств защиты информации, настройки антивирусных средств и

					проведения мониторинга функционирования программно-аппаратных средств защиты информации; - Навыками проведения анализа эффективности программно-аппаратных средств защиты информации и оценивания оптимальности их выбора и режимов функционирования
			С/05.7 Проведение инструментального мониторинга защищенности компьютерных систем и сетей	ПК-3. Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	**ИПК 3.1 Знает:** - Принципы построения компьютерных систем и сетей; - Формальные модели безопасности компьютерных систем и сетей; - Принципы построения систем обнаружения компьютерных атак; - Методы обработки данных мониторинга безопасности компьютерных систем и сетей; - Порядок создания и структура отчета,

					создаваемого по результатам проверок; - Способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; - Криптографические протоколы, применяемые в компьютерных сетях; - Нормативные правовые акты в области защиты информации; - Организационные меры по защите информации **ИПК 3.2 Умеет:** - Формализовывать задачу управления безопасностью компьютерных систем; - Применять инструментальные средства проведения мониторинга защищенности компьютерных систем; - Применять методы анализа защищенности компьютерных систем и сетей; - Структурировать аналитическую информацию для включения в отчет

					ИПК.3.3 Владеет: - Методами измерений, контроля и технических расчётов характеристик программно-аппаратных средств защиты информации, принципами функционирования сетевых протоколов и криптографических алгоритмов; - Навыками анализа компьютерных систем с целью определения уровня защищённости и доверия, прогнозирования возможных путнц развития действий нарушителя информационной безопасности и проведения мониторинга функционирования программно-аппаратных средств защиты информации
	06.033 Специалист по защите информации в автоматизированных системах	С Разработка систем защиты информации автоматизированных систем,	С/01.7 Тестирование систем защиты информации автоматизированных систем	ПК-5. Способен тестировать системы защиты информации	**ИПК 5.1 Знает:** - Принципы построения и функционирования систем и сетей передачи информации;

		используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости			- Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - Основные меры по защите информации в автоматизированных системах; - Особенности защиты информации в автоматизированных системах управления технологическими процессами; - Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам; - Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах **ИПК 5.2 Умеет:** - Анализировать основные характеристики и возможности

					телекоммуникационных систем по передаче информации; - Анализировать основные узлы и устройства современных автоматизированных систем; - Применять действующую нормативную базу в области обеспечения безопасности информации; - Контролировать функционирование технических средств защиты информации; - Восстанавливать (заменять) отказавшие технические средства защиты информации **ИПК.5.3 Владеет:** - Навыками построения плана тестирования для проведения анализа защищённости; - Методиками и навыками проведения тестов для анализа степени защищённости информационной системы

					и её соответствия нормативным требованиям по защите информации
Тип задач профессиональной деятельности: *проектный*					
06 Связь, информационные и коммуникационные технологии (в сфере защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи)	06.033 Специалист по защите информации в автоматизированных системах	C Разработка систем защиты информации автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости	C/02.7 Разработка проектных решений по защите информации в автоматизированных системах	ПК-4. Способен разрабатывать проектные решения по защите информации в автоматизированных системах	**ИПК 4.1 Знает:** - Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов; - Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов; - Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов; - Принципы организации и структуру систем защиты информации программного
		D Формирование требований к защите информации в автоматизированных системах,	D/01.7 Обоснование необходимости защиты информации в автоматизированной системе		

		используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости	D/02.7 Определение угроз безопасности информации, обрабатываемой автоматизированной системой D/03.7 Разработка архитектуры системы защиты информации автоматизированной системы D/04.7 Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации		обеспечения автоматизированных систем; - Основные характеристики технических средств защиты информации от несанкционированного доступа и утечек по техническим каналам; - Принципы формирования политики информационной безопасности в автоматизированных системах; - Основные информационные технологии, используемые в автоматизированных системах; - Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - Виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах;

					- Методы защиты информации от несанкционированного доступа и утечки по техническим каналам; - Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем; - Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; - Принципы формирования политики информационной безопасности в автоматизированных системах; - Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях; - Программно-аппаратные средства обеспечения защиты информации

					автоматизированных систем; - Способы реализации угроз безопасности в автоматизированных системах; - Последствия от нарушения свойств безопасности информации; - Методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем **ИПК 4.2 Умеет:** - Применять действующую нормативную базу в области обеспечения защиты информации; - Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; - Определять методы управления доступом, типы доступа и правила разграничения доступа к

					объектам доступа, подлежащим реализации в автоматизированной системе; - Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; - Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации; - Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем; - Анализировать цели создания автоматизированных систем и задачи, решаемые

					автоматизированными системами; - Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; - Организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем; - Использовать рисковую методологию управления защитой информации в автоматизированной системе; - Производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в

					автоматизированной системе; - Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы; - Систематизировать результаты проведенных исследований; - Анализировать возможные уязвимости информационных систем; - Выявлять известные уязвимости информационных систем; - Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах; - Определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах; - Выявлять уязвимости информационно-технологических ресурсов

					автоматизированных систем; - Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; - Определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие защите; - Определять эффективность применения средств информатизации **ИПК.4.3 Владеет:** - Навыками разработки и внедрения проектных решений по защите информации в автоматизированных системах, включая выбор и настройку средств защиты, а также контроль их эффективности; - Навыками обоснования необходимости защиты

					информации в автоматизированных системах, учитывая особенности их функционирования и требования к безопасности информации; - Навыками разработки и внедрения архитектуры системы защиты информации автоматизированных систем, включая выбор и настройку компонентов системы, а также контроль их взаимодействия и эффективности

Профессиональные компетенции, установленные программой магистратуры, сформированы на основе профессиональных стандартов; анализа требований к профессиональным компетенциям, предъявляемых к выпускникам на рынке труда; обобщения отечественного и зарубежного опыта; проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники.

Совокупность компетенций, установленных программой магистратуры, обеспечивает выпускнику способность осуществлять профессиональную деятельность не менее чем в одной области профессиональной деятельности и сфере профессиональной деятельности и способность решать задачи профессиональной деятельности не менее чем одного типа.

Совокупность запланированных результатов обучения по дисциплинам (модулям) и практикам обеспечивает формирование у выпускника всех компетенций, установленных программой магистратуры.

VII. Методическое обеспечение реализации программы

Учебный план определяет перечень и последовательность освоения дисциплин, практик, промежуточной и государственной итоговой аттестаций, их трудоемкость в зачетных единицах и академических часах, распределение контактной работы обучающихся с преподавателем (в том числе лекционные, практические, лабораторные виды занятий, консультации) и самостоятельной работы обучающихся.

Учебный план и учебный график, определяющий сроки и периоды осуществления видов учебной деятельности и периоды каникул, представлены в Приложении 1.

Матрица соответствия компетенций дисциплинам учебного плана представлена в Приложении 2.

Рабочие программы дисциплин представлены в Приложении 3. Программы практик представлены в Приложении 4.

Для проведения государственной итоговой аттестации разработана Программа подготовки к процедуре защиты и защиты выпускной квалификационной работы (Приложение 5).

Оценочные средства представляются в виде фонда оценочных средств для промежуточной аттестации обучающихся и для государственной итоговой аттестации. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю) или практике входит в состав соответствующей рабочей программы дисциплины (модуля) или программы практики. Фонд оценочных средств для проведения

государственной итоговой аттестации входит в состав Программы подготовки к процедуре защиты и защиты выпускной квалификационной работы.

VIII. Условия реализации программы магистратуры
1. Выполнение общесистемных требований к реализации программы

Университет располагает на законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» по Блоку 1 «Дисциплины (модули)» и Блоку 3 «Государственная итоговая аттестация» в соответствии с учебным планом.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде Университета, включающей несколько электронно-библиотечных систем (электронных библиотек), 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 Университета обеспечивает:

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

– формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» с применением электронного обучения, дистанционных образовательных технологий ЭИОС Университета дополнительно обеспечивает:

– фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения программы магистратуры;

– проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

– взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети «Интернет».

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

2. Выполнение требований к материально-техническому и учебно-методическому обеспечению программы

Помещения для реализации программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» представляют собой учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения, состав которых определен в рабочих программах дисциплин (модулей).

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

Справка о материально-техническом обеспечении программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» представлена в Приложении 6.

Обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам, состав которых определен в рабочих программах дисциплин (модулей).

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

3. Выполнение требований к кадровым условиям реализации программы

Реализация программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» обеспечивается педагогическими работниками

Университета, а также лицами, привлекаемыми Университетом к реализации программы на иных условиях.

Квалификация педагогических работников Университета отвечает квалификационным требованиям, указанным в квалификационных справочниках и (или) профессиональных стандартах (при наличии).

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

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

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

Не менее 60 процентов численности педагогических работников Университета и лиц, привлекаемых к образовательной деятельности Университета на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), имеют 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).

Общее руководство научным содержанием программы магистратуры осуществляется научно-педагогическим работником Университета, имеющим ученую степень (в том числе ученую степень, полученную в иностранном государстве и признаваемую в Российской Федерации), 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 и (или) зарубежных рецензируемых научных журналах и изданиях, а также осуществляющим ежегодную апробацию результатов указанной научно-исследовательской (творческой) деятельности на национальных и международных конференциях.

Сведения о кадровом обеспечении программы представлены в Приложении 7.

4. Выполнение требований к финансовым условиям реализации программы

Финансовое обеспечение реализации программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» осуществляется в объеме не ниже значений базовых нормативов затрат на оказание государственных услуг по реализации образовательных программ высшего образования - программ магистратуры и значений корректирующих коэффициентов к базовым нормативам затрат, определяемых Министерством науки и высшего образования Российской Федерации.

5. Выполнение требований к применяемым механизмам оценки качества образовательной деятельности и подготовки обучающихся по программе

Качество образовательной деятельности и подготовки обучающихся по программе магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» определяется в рамках системы внутренней оценки, а также системы внешней оценки, в которой Университет принимает участие на добровольной основе.

В целях совершенствования программы магистратуры Университет при проведении регулярной внутренней оценки качества образовательной деятельности и подготовки обучающихся по программе магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» привлекает работодателей и (или) их объединения, иных юридических и (или) физических лиц, включая педагогических работников Университет.

В рамках внутренней системы оценки качества образовательной деятельности по программе магистратуры по направлению подготовки

10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» обучающимся предоставляется возможность оценивания условий, содержания, организации и качества образовательного процесса в целом и отдельных дисциплин (модулей) и практик.

Внешняя оценка качества образовательной деятельности по программе магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» в рамках процедуры государственной аккредитации осуществляется с целью подтверждения соответствия образовательной деятельности по программе магистратуры требованиям ФГОС ВО.

Внешняя оценка качества образовательной деятельности и подготовки обучающихся по программе магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» осуществляется в рамках профессионально-общественной аккредитации, проводимой работодателями, их объединениями, а также уполномоченными ими организациями, в том числе иностранными организациями, либо авторизованными национальными профессионально-общественными организациями, входящими в международные структуры, с целью признания качества и уровня подготовки выпускников, отвечающими требованиям профессиональных стандартов (при наличии), требованиям рынка труда к специалистам соответствующего профиля.

IX. Особенности организации образовательного процесса для инвалидов и лиц с ограниченными возможностями здоровья

Образовательная программа магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» предусматривает реализацию организационной модели инклюзивного образования – обеспечения равного доступа к образованию для всех обучающихся с учетом разнообразия особых образовательных потребностей и индивидуальных возможностей.

Университет обеспечивает (при необходимости и наличии соответствующего заявления со стороны лица, признанного инвалидом или имеющего ОВЗ) разработку индивидуальных учебных планов и индивидуальных графиков обучения (как с установленным сроком освоения ОПОП, так и с увеличением срока освоения ОПОП). Срок получения высшего образования при освоении образовательной программы магистратуры по направлению подготовки 10.04.01 Информационная безопасность, профиль «Инженерия безопасности компьютерных систем и сетей» по

индивидуальному учебному плану для инвалидов и лиц с ОВЗ может быть при необходимости увеличен, но не более чем на полгода. Решение о продлении срока обучения принимается на основании личного заявления обучающегося.

При составлении индивидуального графика обучения могут быть предусмотрены различные варианты проведения занятий:

– в академической группе или индивидуально;

– на дому с использованием электронного обучения и дистанционных образовательных технологий (ДОТ).

Выбор методов обучения при составлении индивидуального графика осуществляется, исходя из их доступности для инвалидов и лиц с ОВЗ. В образовательном процессе могут быть использованы социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

При проведении текущего контроля, промежуточной и итоговой аттестации учитываются особенности нозологии инвалидов и лиц с ОВЗ (в том числе проведение контрольных мероприятий в дистанционном формате при необходимости и наличии соответствующего заявления обучающегося).

Университет обеспечивает инвалидов и лиц с ОВЗ специальными материально-техническими средствами обучения (включая специальное программное обеспечение) при наличии обучающихся соответствующих нозологий и получении их заявлений о необходимости предоставления специальных материально-технических средств обучения.

Университет обеспечивает инвалидов и лиц с ОВЗ печатными и электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья, при наличии обучающихся соответствующих нозологий и получении их заявлений о необходимости предоставления специализированных электронных образовательных ресурсов.

Используемые в Университете ЭБС позволяют реализовать следующие возможности инклюзивного образования:

- ЭБС «ЮРАЙТ» (https://urait.ru/) располагает специальной версией для использования слабовидящими обучающимися;

- ЭБС «IPR BOOKS» (http://www.iprbookshop.ru/) имеет специальную адаптивную версию сайта для слабовидящих пользователей. Данная версия предполагает дополнительные инструменты по увеличению размера текста, выбору цветовой гаммы оформления, изменению кернинга, которые позволяют повысить доступность сайта, не прибегая к использованию сторонних ассистивных технологий. Версия сайта ЭБС для слабовидящих

содержит альтернативные форматы печатных материалов (крупный шрифт и аудиофайлы) для обеспечения учебного процесса. Специальный адаптивный ридер на сайте для чтения книг позволяет увеличивать текст до 400% без потери качества.

Форма проведения промежуточной и государственной итоговой аттестации для обучающихся-инвалидов и лиц с ОВЗ устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).

Для выпускников из числа инвалидов и лиц с ОВЗ государственная итоговая аттестация проводится Университетом с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких выпускников. При обращении инвалидов и лиц с ОВЗ к председателю государственной экзаменационной комиссии им предоставляется дополнительное время для подготовки ответа.

При проведении ГИА председатель государственной экзаменационной комиссии обеспечивает соблюдение следующих общих требований:

– проведение ГИА для лиц с ОВЗ в одной аудитории совместно с выпускниками, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для выпускников при прохождении ГИА;

– присутствие в аудитории ассистента (по заявлению выпускника), оказывающего необходимую техническую помощь выпускнику с учетом его индивидуальных особенностей (занять место в аудитории, прочитать доклад, передвигаться, общаться с членами государственной экзаменационной комиссии);

– пользование выпускниками необходимыми им техническими средствами при прохождении ГИА с учетом их индивидуальных особенностей;

– обеспечение возможности беспрепятственного доступа выпускников-инвалидов и имеющих ОВЗ в аудитории, туалетные и другие помещения, а также их пребывание в указанных помещениях.

Выпускники-инвалиды или их законные представители не менее чем за один месяц до начала ГИА подают руководству Университета заявление о необходимости создания им специальных условий при проведении ГИА.