Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 31.08.2023 14:27:01
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

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/
«16» февраля 2023 г.

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

направление подготовки

10.03.01 Информационная безопасность

направленность (профиль)

«Безопасность компьютерных систем»

Уровень образования – бакалавриат

Квалификация (степень): бакалавр

Форма обучения – очная

Год начала обучения – 2023 г.

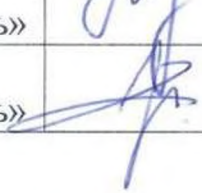
Москва 2023

Лист согласования

Согласовано:

ФИО	Должность / место работы	Подпись, дата
Демидов Дмитрий Григорьевич	Декан факультета информационных технологий	
Гневшев Александр Юрьевич	И.о.зав. кафедрой «Информационная безопасность»	

Разработчики:

ФИО	Должность / место работы	Подпись, дата
Гневшев Александр Юрьевич	И.о.зав. кафедрой «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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» являются:

1. Федеральный государственный образовательный стандарт высшего образования (уровень бакалавриата) по направлению подготовки 10.03.01 Информационная безопасность, утвержденный приказом Министерства образования и науки Российской Федерации от 17.11.2020 № 1427.
2. Профессиональные стандарты:

– 06.032 Специалист по безопасности компьютерных систем и сетей. Утвержден приказом Министерства труда и социальной защиты РФ от 14.09.2022 № 533н;

– 06.033 Специалист по защите информации в автоматизированных системах. Утвержден приказом Министерства труда и социальной защиты РФ от 14.09.2022 г. № 525н.

II. Общие положения

Цель образовательной программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» 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 бакалавриата сформированы требования к результатам ее освоения в виде универсальных, общепрофессиональных и профессиональных компетенций выпускников.

Обучение по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» осуществляется **в очной форме**.

При реализации программы бакалавриата 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» **с использованием сетевой формы не осуществляется**.

Образовательная деятельность по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» осуществляется на государственном языке Российской Федерации – **русском языке**.

Срок получения образования по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» (вне зависимости от применяемых образовательных технологий) в очной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 4 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 1 год.

Объем образовательной программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» составляет 240 з.е. вне зависимости от формы обучения, применяемых образовательных технологий, реализации программы бакалавриата по индивидуальному учебному плану.

Объем программы бакалавриата, реализуемый за один учебный год, составляет не более 70 з.е. вне зависимости от формы обучения, применяемых образовательных технологий, реализации программы бакалавриата 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, могут осуществлять профессиональную деятельность:

01 Образование и наука (в сфере научных исследований);

06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере);

12 Обеспечение безопасности (в сфере эксплуатации технических и программно-аппаратных средств защиты информации);

сфера обороны и безопасности;

сфера правоохранительной деятельности.

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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» ориентирована на следующие области профессиональной деятельности (ОПД):

06 Связь, информационные и коммуникационные технологии (в сфере проектирования, разработки, внедрения и эксплуатации информационных систем, управления их жизненным циклом).

В рамках освоения программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» выпускники готовятся к решению задач профессиональной деятельности следующих типов:

- эксплуатационный;
- проектно-технологический;
- экспериментально-исследовательский;
- организационно-управленческий.

Программа бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных

систем» ориентирована на следующие объекты профессиональной деятельности выпускников:

– системы информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере;

– технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;

– процессы управления информационной безопасностью защищаемых объектов.

Программа бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем», представлен в таблице 1.

Таблица 1 – Перечень обобщённых трудовых функций и трудовых функций, соответствующих профессиональной деятельности выпускника программы бакалавриата 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем»

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
06.032 Специалист по безопасности компьютерных систем и сетей / Обеспечение безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности	B	Администрирование средств защиты информации в компьютерных системах и сетях	6	Администрирование подсистем защиты информации в операционных системах	B/01.6	6
				Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	B/02.6	6
				Администрирование средств защиты информации прикладного и системного программного обеспечения	B/03.6	6
06.033 Специалист по защите информации в автоматизированных системах / Обеспечение безопасности информации в автоматизированных системах, используемых в том числе на объектах критической информационной	B	Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость	6	Диагностика систем защиты информации автоматизированных систем	B/01.6	6
				Администрирование систем защиты информации автоматизированных систем	B/02.6	6

инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости		присвоения им категорий значимости, в процессе их эксплуатации		Управление защитой информации в автоматизированных системах	B/03.6	6
				Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций	B/04.6	6
				Мониторинг защищенности информации в автоматизированных системах	B/05.6	6
				Аудит защищенности информации в автоматизированных системах	B/06.6	6
				Установка и настройка средств защиты информации в автоматизированных системах	B/07.6	6
				Разработка организационно-распорядительных документов по защите информации в автоматизированных системах	B/08.6	6

				Анализ уязвимостей внедряемой системы защиты информации	B/09.6	6
				Внедрение организационных мер по защите информации в автоматизированных системах	B/10.6	6

V. Структура и объем образовательной программы

Структура программы бакалавриата включает следующие блоки.

Блок 1 «Дисциплины (модули)».

Блок 2 «Практика».

Блок 3 «Государственная итоговая аттестация».

Таблица 2 - Структура программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем»

Структура программы бакалавриата		Объем программы бакалавриата и её блоков в з.е.
Блок 1	Дисциплины (модули)	207
Блок 2	Практика	27
Блок 3	Государственная итоговая аттестация	6
Объем программы бакалавриата		240

Программа бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» обеспечивает реализацию дисциплин (модулей) по философии, истории России, иностранному языку, безопасности жизнедеятельности в рамках Блока 1 «Дисциплины (модули)».

Программа бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» обеспечивает реализацию дисциплин (модулей) по физической культуре и спорту: в объеме 2 з.е. в рамках Блока 1 «Дисциплины (модули)»; в объеме 328 академических часов, которые являются обязательными для освоения, не переводятся в з.е. и не включаются в объем программы бакалавриата, в рамках элективных дисциплин (модулей) в очной форме обучения. Дисциплины (модули) по физической культуре и спорту реализуются в порядке, установленном Университетом. Для инвалидов и лиц с ОВЗ Университет устанавливает особый порядок освоения дисциплин (модулей) по физической культуре и спорту с учетом состояния их здоровья.

В блок 2 «Практика» входят учебная и производственная практики.

Типы учебной практики:

- ознакомительная практика.

Типы производственной практики:

- технологическая практика;
- преддипломная практика.

В Блок 3 «Государственная итоговая аттестация» входят:

– подготовка к процедуре защиты и защита выпускной квалификационной работы.

Программа бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» обеспечивает обучающимся возможность освоения элективных дисциплин (модулей) и факультативных дисциплин (модулей). Факультативные дисциплины (модули) не включаются в объем программы бакалавриата.

Программа бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» включает обязательную часть и часть, формируемую участниками образовательных отношений. Объем обязательной части без учета объема государственной итоговой аттестации составляет более 65 процентов общего объема программы бакалавриата.

Университет предоставляет инвалидам и лицам с ОВЗ (по их заявлению) возможность обучения по программе бакалавриата, 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» составляет в очной форме обучения более 50 процентов.

VI. Планируемые результаты освоения образовательной программы

В результате освоения программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» у выпускника должны быть сформированы следующие компетенции, установленные программой бакалавриата (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	УК-1. Способен осуществлять поиск, критический анализ	ИУК-1.1. Анализирует задачу, выделяя ее базовые составляющие

мышление	и синтез информации, применять системный подход для решения поставленных задач	ИУК-1.2. Осуществляет поиск, критически оценивает, обобщает, систематизирует и ранжирует информацию, требуемую для решения поставленной задачи ИУК-1.3. Рассматривает и предлагает рациональные варианты решения поставленной задачи, используя системный подход, критически оценивает их достоинства и недостатки
Разработка и реализация проектов	УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	ИУК-2.1.Формулирует совокупность задач в рамках поставленной цели проекта, решение которых обеспечивает ее достижение ИУК-2.2. Определяет связи между поставленными задачами, основными компонентами проекта и ожидаемыми результатами его реализации ИУК-2.3. Выбирает оптимальные способы планирования, распределения зон ответственности, решения задач, анализа результатов с учетом действующих правовых норм, имеющихся условий, ресурсов и ограничений, возможностей использования
Командная работа и лидерство	УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	ИУК-3.1. Определяет свою роль в команде, исходя из стратегии сотрудничества для достижения поставленной цели, учитывая особенности поведения и интересы других участников команды ИУК-3.2. Планирует и анализирует последствия личных действий, адекватно оценивает идеи и предложения других участников для достижения поставленной цели в командной работе ИУК-3.3. Осуществляет обмен информацией, знаниями и опытом с членами команды, соблюдая установленные нормы и правила социального взаимодействия, несет личную ответственность за свой вклад в результат командной работы
Коммуникация	УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской	ИУК-4.1. Учитывает особенности деловой коммуникации на государственном и иностранном языках в зависимости от особенностей вербальных и невербальных средств общения ИУК-4.2. Умеет вести обмен деловой информацией в устной и письменной формах на государственном и

	Федерации и иностранном (ых) языке (ах)	иностранном языках с учетом своеобразия стилистики официальных и неофициальных писем, а также социокультурных различий в формате корреспонденции ИУК-4.3. Выполняет перевод профессиональных текстов с иностранного языка на государственный язык РФ и с государственного языка РФ на иностранный
Межкультурное взаимодействие	УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	ИУК-5.1. Анализирует и интерпретирует события, современное состояние общества, проявления его межкультурного разнообразия в социально-историческом, этическом и философском контекстах ИУК-5.2. Осознает систему общечеловеческих ценностей, понимает значение для развития цивилизаций исторического наследия и социокультурных традиций различных социальных групп, этносов и конфессий, а также мировых религий, философских и этических учений ИУК-5.3. Взаимодействует с людьми с учетом социокультурных особенностей в целях успешного выполнения профессиональных задач и социальной интеграции
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	ИУК-6.1. Использует инструменты и методы управления временем при выполнении конкретных задач, проектов, при достижении поставленных целей ИУК-6.2. Определяет приоритеты собственной деятельности, личностного развития и профессионального роста ИУК-6.3. Демонстрирует готовность к построению профессиональной карьеры и определению стратегии профессионального развития на основе оценки требований рынка труда, предложений рынка образовательных услуг и с учетом личностных возможностей и предпочтений
	УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и	ИУК-7.1. Грамотно выбирает методы здоровьесбережения для поддержания здорового образа жизни с учетом физиологических особенностей организма и условий реализации профессиональной деятельности ИУК-7.2. Поддерживает оптимальный уровень физической нагрузки для

	профессиональной деятельности	обеспечения полноценной социальной и профессиональной деятельности ИУК-7.3. Соблюдает нормы здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности
Безопасность жизнедеятельности	УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	ИУК-8.1. Анализирует и идентифицирует факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений), а также опасные и вредные факторы в рамках осуществляемой деятельности ИУК-8.2. Понимает важность поддержания безопасных условий труда и жизнедеятельности, сохранения природной среды для обеспечения устойчивого развития общества, в том числе при угрозе возникновения опасных или чрезвычайных ситуаций и военных конфликтов ИУК-8.3. Разъясняет правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения и военных конфликтов, описывает способы участия в восстановительных мероприятиях
Экономическая культура, в том числе финансовая грамотность	УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	ИУК-9.1. Понимает базовые принципы функционирования макроэкономики и экономического развития, цели и виды участия государства в экономике ИУК-9.2. Представляет основные закономерности функционирования микроэкономики и факторы, обеспечивающие рациональное использование ресурсов и достижение эффективных результатов деятельности ИУК-9.3. Применяет методы экономического и финансового планирования для достижения личных финансовых целей, использует адекватные поставленным целям финансовые инструменты управления личным бюджетом, оптимизирует собственные финансовые риски
Гражданская позиция	УК-10. Способен формировать нетерпимое отношение к	ИУК-10.1. Понимает сущность экстремизма, терроризма, коррупции, опасность их разрушительного влияния

	проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	на социальные, экономические и иные отношения в гражданском обществе ИУК-10.2. Умеет применять правовые нормы, обеспечивающие противодействие экстремизму, терроризму, коррупции и профилактику их проявлений в сфере профессиональной деятельности ИУК-10.3. Владеет средствами формирования нетерпимого отношения к проявлениям экстремизма, терроризма и коррупционного поведения и противодействия им в профессиональной деятельности

Таблица 4 - Общепрофессиональные компетенции выпускников и индикаторы их достижения

Категория компетенций	Код и наименование компетенции	Код и содержание индикатора достижения компетенции
	ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИОПК-1.1 Знает основные понятия информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных; ИОПК-1.2. Умеет использовать программные и аппаратные средства персонального компьютера; ИОПК-1.3. Владеет навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.).
	ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ИОПК-2.1 Знает информационно-коммуникационные технологии, программные средства системного и прикладного назначения; ИОПК-2.2. Умеет применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач

		профессиональной деятельности ИОПК-2.3.Владеет навыками применения информационно-коммуникационных технологий, программными средствами системного и прикладного назначения, в том числе отечественного производства, для решения задач.
	ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ИОПК-3.1. Знает основные понятия и методы математического анализа, аналитической геометрии, линейной алгебры, теории функций комплексного переменного, математические методы обработки экспериментальных данных, основные понятия и методы математической логики и теории алгоритмов, основные понятия, составляющие предмет дискретной математики, основные методы решения задач профессиональной области с применением дискретных моделей, основные понятия и методы теории вероятностей и математической статистики, математические методы обработки экспериментальных данных, основные понятия теории информации (энтропия, взаимная информации, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации, основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума, понятие пропускной способности канала связи, прямую и обратную теоремы кодирования, основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды – линейные, циклические, БЧХ, Хэмминга); ИОПК-3.2. -Умеет строить

		математические модели задач профессионально области, применять стандартные методы дискретной математики к решению типовых задач, осуществлять поиск научной информации и работу с реферативной, справочной, периодической и монографической литературой по различным областям дискретной математики, использовать математические методы и модели для решения прикладных задач, вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информация, пропускная способность), решать типовые задачи кодирования и декодирования, использовать математические методы и модели для решения прикладных задач, работать с научно-технической литературой по тематике дисциплины; ИОПК-3.3. Владеет методами количественного анализа процессов обработки, поиска и передачи информации, навыками самостоятельного решения комбинаторных задач, навыками нахождения различных параметров и представлений булевых функций, навыками вычисления параметров графов, методами количественного анализа процессов обработки, поиска и передачи информации, основами построения математических моделей текстовой информации и моделей систем передачи информации, навыками применения математического аппарата для решения прикладных теоретико-информационных задач.
	ОПК-4. Способен применять необходимые физические законы и модели для решения	ИОПК-4.1.Знает особенности физических эффектов и явлений, используемых для обеспечения

	задач профессиональной деятельности	информационной безопасности; ИОПК-4.2. Умеет применять основные законы физики при решении практических задач. ИПК-4.3. Владеет: - методами теоретического исследования физических явлений и процессов; навыками проведения физического эксперимента и обработки его результатов.
	ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ИОПК-5.1. Знает основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; ИОПК-5.2. Умеет применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, пользоваться нормативными документами по защите информации; ИОПК-5.3. Владеет навыками работы с нормативными правовыми актами.
	ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИОПК-6.1 Знает защитные механизмы и средства обеспечения безопасности операционных систем, основные виды политик управления доступом и информационными потоками в компьютерных системах, организацию работы и нормативные акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые

		акты в области обеспечения информационной безопасности; ИОПК-6.2. Умеет пользоваться нормативными документами в области информационной безопасности; ИОПК-6.3. Владеет навыками работы с нормативными правовыми актами.
	ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ИОПК-7.1. Знает современные средства разработки и анализа программного обеспечения на языках высокого уровня, методы программирования и разработки эффективных алгоритмов решения прикладных задач, базовые структуры данных, основные алгоритмы сортировки и поиска и способы их эффективной реализации, основы администрирования операционных систем и вычислительных сетей, эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы; ИОПК-7.2. Умеет выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах, составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные, формализовать поставленную задачу, выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах, устанавливать и осуществлять первичную настройку одной из операционных систем; ИОПК-7.3. Владеет навыками разработки программ на языке программирования высокого уровня, способами оценки сложности работы алгоритмов,

		основными подходами к организации процесса разработки программного обеспечения.
	ОПК-8. Способен осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ИОПК-8.1. Знает необходимые нормативно-методические документ ИОПК-8.1. Умеет составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем. ИОПК-8.3. Владеет методами работы с научно- технической литературы, нормативных и методических документов.
	ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИОПК-9.1. Знает средства криптографической и технической защиты информации для решения задач профессиональной деятельности; ИОПК-9.2. Умеет применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности. ИОПК-9.3. Владеет средствами криптографической и технической защиты информации для решения задач профессиональной деятельности
	ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИОПК-10.1. Знает принципы формирования политики информационной безопасности в информационных системах; ИОПК-10.2. Умеет разрабатывать частные политики информационной безопасности информационных систем, определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, управлять процессом их реализации на объекте защиты. ИОПК-10.3. Владеет методами работы технического специалиста и поддержкой выполнения комплекса мер по обеспечению информационной

		безопасности, управлением процессом их реализации на объекте защиты
	ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов	ИОПК-11.3. Владеет навыками проведения физического эксперимента и обработки его результатов, методами расчета и инструментального контроля показателей технической защиты информации.
	ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ИОПК-12.1. Знает основные угрозы безопасности информации и модели нарушителя в информационных системах; ИОПК-12.2. Умеет разрабатывать модели угроз и нарушителей информационной безопасности информационных систем, определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, выявлять уязвимости информационно-технологических ресурсов информационных систем; ИОПК-12.3. Владеет навыками анализа информационной инфраструктуры информационной системы и ее безопасности, методами выявления угроз информационной безопасности информационных систем.
	ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	ИОПК-13.3. Демонстрирует уважительное отношение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения.
направленность (профиль) Безопасность компьютерных систем		
	ОПК-1.1. Способен разрабатывать и реализовывать	ИОПК-1.1.1. Знает формальные модели политик безопасности,

	политики управления доступом в компьютерных системах	политик управления доступом и информационными потоками в компьютерных системах; ИОПК-1.1.2. Умеет применять формальные модели для разработки политик безопасности, политик управления доступом; ИОПК-1.1.3. Владеет навыками создания формальных моделей управления доступом.
	ОПК-1.2. Способен администрировать средства защиты информации в компьютерных системах и сетях	ИОПК-1.2.1.Знает принципы организации информационных систем в соответствии с требованиями по защите информации, криптографические стандарты и как их использовать в информационных системах; ИОПК-1.2.2.Умеет развертывать, конфигурировать и настраивать вычислительные сети, формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; ИОПК-1.2.3.Владеет навыками использования типовых криптографических алгоритмов.
	ОПК-1.3. Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	ИОПК-1.3.1. Знает архитектуру систем баз данных, основные модели данных, этапы и методы проектирования; ИОПК-1.3.2.Умеет применять языки программирования и инструментальные средства в профессиональной деятельности, обосновывать выбор необходимых инструментальных средства для создания, функционирования и защиты базы данных на предприятии; ИОПК-1.3.3.Владеет методами и средствами построения баз данных, демонстрировать способность и готовность к

		эксплуатации и администрированию баз данных с учетом требований по обеспечению информационной безопасности.
	ОПК-1.4. Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ИОПК-1.4.1. Знает основные методы управления информационной безопасностью; ИОПК-1.4.2.Умеет оценивать информационные риски в информационных системах, разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; ИОПК-1.4.3.Владеет методами управления информационной безопасностью информационных систем, методами оценки информационных рисков.

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: эксплуатационный					
06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)	06.033 Специалист по защите информации в автоматизированных системах	B/6 Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	B/08.6 Установка и настройка средств защиты информации в автоматизированных системах	ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	ИПК-1.1. Знает современные виды информационного взаимодействия и обслуживания, принципы и методы противодействия несанкционированному информационному воздействию на вычислительные сети и системы передачи информации, основные задачи и понятия криптографии, требования к шифрам и основные характеристики шифров, модели шифров и математические методы их исследования, принципы построения криптографических алгоритмов;

					ИПК-1.2. Умеет использовать и настраивать программно-аппаратные средства защиты информации, проводить анализ показателей качества сетей и систем связи ИПК-1.3. Владеет навыками по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации
	06.033 Специалист по защите информации в автоматизированных системах	B/6 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	B/01.6 Диагностика систем защиты информации автоматизированных систем B/05.6 Мониторинг защищенности информации в автоматизированных системах; B/06.6 Аудит защищенности информации в автоматизированных системах	ПК-2. Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ИПК-2.1. Знает организацию работы и нормативные правовые акты по аттестации объектов информатизации, методы аттестации уровня защищенности информационных систем; ИПК-2-2. Умеет участвовать в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

					владеет методиками проверки защищенности объектов информатизации на соответствие нормативных документов.
06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)	06.033 Специалист по защите информации в автоматизированных системах	B/6 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	B/03.6 Управление защитой информации в автоматизированных системах; B/04.6 Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций	ПК-3. Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ИПК-3.1. Знает методы и средства контроля эффективности технической защиты информации; ИПК-3.2. Умеет контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; ИПК-3.3. Владеет навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем, навыками участия в экспертизе состояния защищенности информации на объекте защиты.
Тип задач профессиональной деятельности: проектно-технологический					

06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)	06.033 Специалист по защите информации в автоматизированных системах	B/6 Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	B/08.6 Разработка организационно-распорядительных документов по защите информации в автоматизированных системах	ПК-4. Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ИПК-4.1. Знает свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления, задачи органов защиты информации на предприятиях, порядок организации работы и нормативные правовые акты по сертификации средств защиты информации; ИПК-4.2. Умеет квалифицированно исследовать состав документации предприятия (организации), разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; владеет методами формирования требований по защите информации.
Тип задач профессиональной деятельности: экспериментально-исследовательский					

06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)	06.033 Специалист по защите информации в автоматизированных системах	B/6 Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	B/09.6 Анализ уязвимостей внедряемой системы защиты информации	ПК-5. Способен принимать участие в проведении экспериментальных исследований системы защиты информации	ИПК-5.1. Знает технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; ИПК-5.2. Умеет анализировать и оценивать угрозы информационной безопасности объекта, проводить мониторинг угроз безопасности информационных систем; ИПК-5.3. Владеет методами и средствами выявления угроз безопасности, методами технической защиты информации, методами формирования требований по защите информации, методами мониторинга и аудита угроз информационной безопасности информационных систем.

Тип задач профессиональной деятельности: организационно-управленческий					
06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в	06.033 Специалист по защите информации в автоматизированных системах	B/6 Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	B/10.6 Внедрение организационных мер по защите информации в автоматизированных системах	ПК-6. Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ИПК-6.1. Знает принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); ИПК-6.2. владеет методами организации и управления деятельность служб защиты информации на предприятии.

информационной сфере)	06.032 Специалист по безопасности компьютерных систем и сетей	B/6 Администрирование средств защиты информации в компьютерных системах и сетях	B/01.6 Администрирование подсистем защиты информации в операционных системах в компьютерных сетях B/02.6 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях B/03.6 Администрирование средств защиты информации прикладного и системного программного обеспечения	ПК-7. Способен организовывать работу малого коллектива исполнителей в профессиональной деятельности	ИПК-7.1. Знает основные понятия и методы в области управленческой деятельности, содержание управленческой работы руководителя подразделения; ИПК-7.2. Умеет осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; ИПК-7.3. Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения.
	06.033 Специалист по защите информации в автоматизированных системах	B/6 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	B/02.6 Администрирование систем защиты информации автоматизированных систем	ПК-8. Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными	ИПК-8.1. Знает правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях,

				методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации; ИПК-8.2. Владеет навыками организации и обеспечения режима секретности.

Профессиональные компетенции, установленные программой бакалавриата, 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 / иных источников.

Совокупность компетенций, установленных программой бакалавриата, 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 бакалавриата.

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 выполнения и защиты выпускной квалификационной работы (Приложение 5).

Рабочая программа воспитания и Календарный план воспитательной работы представлены в Приложении 8.

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 выполнения и защиты выпускной квалификационной работы.

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

Университет располагает на законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» с применением электронного обучения, дистанционных образовательных технологий ЭИОС Университета дополнительно обеспечивает:

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

– 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» 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).

Более 70 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).

Более 3 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 более 55 процентов от общего количества лиц, привлекаемых к реализации программы.

Более 50 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).

Сведения о кадровом обеспечении программы представлены в Приложении 7.

4. Выполнение требований к финансовым условиям реализации программы

Финансовое обеспечение реализации программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» осуществляется в объеме не ниже значений базовых нормативов затрат на оказание государственных услуг по реализации образовательных программ высшего образования - программ бакалавриата 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» определяется в рамках системы внутренней оценки, а также системы внешней оценки, в которой Университет принимает участие на добровольной основе.

В целях совершенствования программы бакалавриата Университет при проведении регулярной внутренней оценки качества образовательной деятельности и подготовки обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» в рамках процедуры государственной аккредитации осуществляется с целью

подтверждения соответствия образовательной деятельности по программе бакалавриата требованиям ФГОС ВО.

Внешняя оценка качества образовательной деятельности и подготовки обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем» по индивидуальному учебному плану для инвалидов и лиц с ОВЗ может быть при необходимости увеличен, но не более чем на один год. 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.

Освоение дисциплин «Физическая культура и спорт» и «Элективные дисциплины по физической культуре и спорту» в рамках образовательной программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных

систем» обучающимися-инвалидами и лицами с ОВЗ осуществляется в соответствии с рекомендациями учреждений медико-социальной экспертизы на основании соблюдения принципов здоровьесбережения и адаптивной физической культуры. В зависимости от нозологии обучающегося и степени ограниченности возможностей в соответствии с рекомендациями службы медико-социальной экспертизы или психолого-медико-педагогической комиссии, занятия для студентов с ОВЗ могут быть организованы в следующих видах:

– подвижные занятия адаптивной физической культурой в спортивных, тренажерных залах или на открытом воздухе;

– занятия по настольным, интеллектуальным видам спорта;

– лекционные занятия по тематике здоровьесбережения.

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.