Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 31.05.2024 10:50:10
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/
«__15__»___февраля____ 2024 г.

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

специальность

10.05.03 Информационная безопасность автоматизированных систем

специализация №5

Безопасность открытых информационных систем

Уровень образования – специалитет

Квалификация – специалист по защите информации

Форма обучения – очная

Год начала обучения – 2024 г.

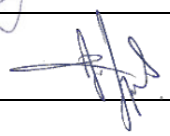
Москва 2024

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 высшего образования

Основой при разработке образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» являются:

1. Федеральный государственный образовательный стандарт высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденный приказом Министерства науки и высшего образования Российской Федерации от 26.11.2020 № 1457.
2. Профессиональные стандарты:

– 06.032 Специалист по безопасности компьютерных систем и сетей. Утвержден приказом Минтруда России от 14.09.2022 № 533н;

– 06.033 Специалист по защите информации в автоматизированных системах. Утвержден приказом Минтруда России от 14.09.2022 № 525н.

II. Общие положения

Цель образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных 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 со специальностью.

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

Обучение по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» осуществляется **в очной форме**.

При реализации программы специалитета 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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» **с использованием сетевой формы не осуществляется**.

Образовательная деятельность по программе специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» осуществляется на государственном языке Российской Федерации – **русском языке**.

Срок получения образования по программе специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» (вне зависимости от применяемых образовательных технологий) в очной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 5,5 лет.

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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» составляет 330 з.е. вне зависимости от формы обучения, применяемых образовательных технологий, реализации программы специалитета по индивидуальному учебному плану.

Объем программы специалитета, реализуемый за один учебный год, составляет не более 70 з.е. вне зависимости от формы обучения, применяемых образовательных технологий, реализации программы специалитета 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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, могут осуществлять профессиональную деятельность:

01 Образование и наука (в сфере научных исследований);

06 Связь, информационные и коммуникационные технологии (в сфере обеспечения безопасности информации в автоматизированных системах);

12 Обеспечение безопасности (в сфере обеспечения безопасности информации в автоматизированных системах, обладающих информационно-технологическими ресурсами, подлежащими защите);

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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ориентирована на следующие области профессиональной деятельности (ОПД):

06 Связь, информационные и коммуникационные технологии (в сфере обеспечения безопасности информации в автоматизированных системах).

В рамках освоения программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» выпускники готовятся к решению задач профессиональной деятельности следующих типов:

- проектный;
- контрольно-аналитический;
- организационно-управленческий.

Программа специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ориентирована на следующие объекты профессиональной деятельности выпускников:

– 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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных 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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем», представлен в таблице 1.

Таблица 1 – Перечень обобщённых трудовых функций и трудовых функций, соответствующих профессиональной деятельности выпускника программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных 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	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	
				Администрирование средств защиты информации прикладного и системного программного обеспечения	B/03.6	
	C	Оценивание уровня безопасности компьютерных систем и сетей	7	Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации в компьютерных системах и сетях	C/01.7	7
				Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей	C/02.7	
				Проведение анализа	C/03.7	

				безопасности компьютерных систем		
				Проведение сертификации программно-аппаратных средств защиты информации	С/04.7	
				Проведение инструментального мониторинга защищенности компьютерных систем и сетей	С/05.7	
				Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях	С/06.7	
06.033 Специалист по защите информации в автоматизированных системах	В	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	6	Диагностика систем защиты информации автоматизированных систем	В/01.6	6
				Администрирование систем защиты информации автоматизированных систем	В/02.6	
				Управление защитой информации в автоматизированных системах	В/03.6	
				Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций	В/04.6	
				Мониторинг защищенности информации в автоматизированных системах	В/05.6	
				Мониторинг защищенности информации в автоматизированных системах	В/06.6	

	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	Тестирование систем защиты информации автоматизированных систем	C/01.7	7
				Разработка проектных решений по защите информации в автоматизированных системах	C/02.7	
				Разработка эксплуатационной документации на системы защиты информации автоматизированных систем	C/03.7	
				Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем	C/04.7	
	D	Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости	7	Обоснование необходимости защиты информации в автоматизированной системе	D/01.7	7
				Определение угроз безопасности информации, обрабатываемой автоматизированной системой	D/02.7	
				Разработка архитектуры системы защиты информации автоматизированной системы	D/03.7	
				Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации	D/04.7	

V. Структура и объем образовательной программы

Структура программы специалитета включает следующие блоки:

Блок 1 «Дисциплины (модули)».

Блок 2 «Практика».

Блок 3 «Государственная итоговая аттестация».

Таблица 2 - Структура программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем»

Структура программы специалитета		Объем программы специалитета и её блоков в з.е.
Блок 1	Дисциплины (модули)	282
Блок 2	Практика	42
Блок 3	Государственная итоговая аттестация	6
Объем программы специалитета		330

Программа специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» обеспечивает реализацию дисциплин (модулей) по философии, иностранному языку, безопасности жизнедеятельности в рамках Блока 1 «Дисциплины (модули)».

Программа специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» обеспечивает реализацию дисциплины (модуля) «История России» в объеме 4 з.е., при этом объем контактной работы обучающихся с педагогическими работниками составляет в очной форме обучения более 80 процентов объема, отводимого на реализацию указанной дисциплины (модуля).

Программа специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных 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 специалитета, 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:

– проектно-технологическая практика;
– экспериментально-исследовательская практика.

Типы производственной практики:

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

В Блок 3 «Государственная итоговая аттестация» входят:

– подготовка к процедуре защиты и защита выпускной квалификационной работы.

Программа специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» обеспечивает обучающимся возможность освоения элективных дисциплин (модулей) и факультативных дисциплин (модулей). Факультативные дисциплины (модули) не включаются в объем программы специалитета.

Программа специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» включает обязательную часть и часть, формируемую участниками образовательных отношений. Объем обязательной части без учета объема государственной итоговой аттестации составляет более 50 процентов общего объема программы специалитета.

Университет предоставляет инвалидам и лицам с ОВЗ (по их заявлению) возможность обучения по программе специалитета, 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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» составляет в очной форме обучения более 50 процентов.

VI. Планируемые результаты освоения образовательной программы

В результате освоения программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» у выпускника должны быть сформированы следующие компетенции, установленные программой специалитета (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 междисциплинарных 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 и образования в течение всей жизни	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.
	УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	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 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	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

	угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	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-11. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-11.1. Понимает сущность экстремизма, терроризма, коррупции, опасность их разрушительного влияния на социальные, экономические и иные отношения в гражданском обществе; ИУК-11.2. Умеет применять правовые нормы, обеспечивающие противодействие экстремизму, терроризму, коррупции и профилактику их проявлений в сфере профессиональной деятельности; ИУК-11.3. 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 программные средства системного и прикладного назначений, 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 математические методы, необходимые 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 анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ИОПК-4.1 Знает: - Основные законы механики; - Основные законы термодинамики и молекулярной физики; - Основные законы электричества и магнетизма; - Основы квантовой физики и физики твердого тела; - Основы теории колебаний и волн, оптики; - Физические явления и эффекты, используемые при обработке, хранении, передаче, уничтожении и защиты информации. ИОПК-4.2 Умеет: - строить математические модели физических явлений и процессов; - решать типовые прикладные физические задачи; - анализировать и применять физические явления и эффекты для решения практических задач

		обеспечения информационной безопасности; - применять математические методы исследования моделей шифров; - основы физической защиты объектов информатизации. ИОПК-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	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 автоматизированных системах 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 создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	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 применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	ИОПК-8.1. Знает методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах; ИОПК-8.2. Умеет применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах ОПК-8.3 Владеет методами научных исследований при проведении разработок в области защиты информации в автоматизированных системах
	ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ИОПК-9.1. Знает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации; ИОПК-9.2 Умеет решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий. ИОПК-9.3. Владеет методами решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации
	ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ИОПК-10.1. Знает средства криптографической и технической защиты информации для решения задач профессиональной деятельности; ИОПК-10.2. Умеет применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности. ИОПК-10.3. Владеет средствами криптографической и технической

		защиты информации для решения задач профессиональной деятельности
	ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ИОПК-11.1. Знает программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах. системах управления базами данных, компьютерных сетях. ИОПК-11.2. Умеет проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы. ИОПК-11.3. Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения; навыками работы с нормативными правовыми актами; навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ.
	ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ИОПК-12.1. Знает принципы построения и функционирования, примеры реализаций современных операционных систем; основные протоколы сетей ЭВМ; основные задачи и понятия криптографии; архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем; - ИОПК-12.2. Владеет методами сбора, обработки, анализа и систематизации научно-

		технической информации в области ЭВМ и систем с применением современных информационных технологий; методами, способами, средствами, последовательностью и содержанием этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; использовать в практической деятельности правовые знания; разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации. ИОПК-12.3. Владеет навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем; навыками анализа и синтеза структурных и функциональных схем, защищенных автоматизированных информационных систем; анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; - навыками использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры; навыками работы с программными средствами схемотехнического моделирования.
	ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем,	ИОПК-13.1. Знает методы и средства диагностики и тестирования систем защиты информации автоматизированных систем;

	проводить анализ уязвимостей систем защиты информации автоматизированных систем	ИОПК-13.2. Умеет проводить анализ уязвимостей систем защиты информации автоматизированных систем. ИОПК-13.3. Владеет способами организации и проведения диагностики и тестирования систем защиты информации автоматизированных систем и проведением анализа уязвимости.
	ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	ИОПК-14.1. Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах. ИОПК-14.2. Умеет разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем. ИОПК-14.3. Владеет методами формирования требований по защите информации; методами и технологиями проектирования,

		моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; - методами и средствами технической защиты информации.
	ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ИОПК-15.1. Знает технические каналы утечки информации. ИОПК-15.2. Умеет проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации. ИОПК-15.3. Владеет методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.
Направленность (профиль) «Безопасность открытых информационных систем»		
	ОПК-1.1. Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	ИОПК-1.1.1 Знает: - основные угрозы безопасности информации и модели нарушителя в открытых информационных системах; - принципы формирования политики информационной безопасности в автоматизированных системах. ИОПК-1.1.2. Умеет: - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - разрабатывать модели угроз и нарушителей информационной безопасности открытых информационных систем; - разрабатывать частные политики информационной безопасности информационной безопасности открытых информационных систем. ИОПК-1.1.3. Владеет: навыками анализа информационной инфраструктуры открытых информационных систем и безопасности.
	ОПК-1.2. Способен разрабатывать и эксплуатировать системы защиты информации	ИОПК-1.2.2 Умеет: - разрабатывать и эксплуатировать системы защиты

	открытых информационных систем	информации открытых информационных систем.
	ОПК-1.3. Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ИОПК-1.3.2. Умеет: - осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах.

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: проектный					
06 Связь, информационные и коммуникационные технологии (в сфере обеспечения безопасности информации в автоматизированных системах)	06.032 Специалист по безопасности компьютерных систем и сетей	B/6 Администрирование средств защиты информации в компьютерных системах и сетях	B/03.6 Администрирование средств защиты информации прикладного и системного программного обеспечения	ПК-1 Способность создавать и исследовать модели автоматизированных систем.	ИПК-1.1. Знает: модели шифров и математические методы их исследования; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные характеристики сигналов электросвязи, спектры и виды модуляции; эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации; требования к шифрам и основные характеристики

					шифров; модели шифров и математические методы их исследования. ИПК-1.2. Умеет: разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений. ИПК-1.3. Владеет: навыками математического моделирования в криптографии; методами и технологиями проектирования, моделирования, исследования

					автоматизированных систем и подсистем безопасности автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.
	06.032 Специалист по безопасности	С/7 Оценивание уровня безопасности компьютерных систем и сетей	С/03.7 Проведение анализа безопасности	ПК-2. Способность проводить анализ защищенности	ИПК-2.1. Знает: требования к шифрам и основные характеристики

	компьютерных систем и сетей		компьютерных систем	автоматизированных систем	шифров; модели шифров и математические методы их исследования; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; технические каналы утечки информации; возможности технических средств перехвата информации ИПК-2.2. Умеет организовывать защиту информации от утечки по техническим каналам на объектах информатизации ИПК-2.3. Владеет: навыками организации и обеспечения режима секретности.
	06.032 Специалист по безопасности	С/7 Оценивание уровня безопасности	С/05.7 Проведение инструментального мониторинга	ПК-3 Способность разрабатывать модели угроз и	ИПК-3.1. Знает: основные угрозы безопасности

	компьютерных систем и сетей 06.033 Специалист по защите информации в автоматизированных системах	компьютерных систем и сетей С/6 Внедрение систем защиты информации автоматизированных систем	защищенности компьютерных систем и сетей С/03.6Анализ уязвимостей внедряемой системы защиты информации	модели нарушителя информационной безопасности автоматизированной системы	информации и модели нарушителя в автоматизированных системах; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах. ИПК-3.2.Умеет: разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности

					автоматизированных систем; анализировать и оценивать угрозы информационной безопасности объекта. ИПК-3.3. Владеет навыками организации и обеспечения режима защиты от угроз информационной безопасности объекта.
	06.032 Специалист по безопасности компьютерных систем и сетей	C/7 Оценивание уровня безопасности компьютерных систем и сетей	C/06.7 Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-4. Способность проводить анализ рисков информационной безопасности автоматизированной системы	ИПК-4.1. Знает: требования к шифрам и основные характеристики шифров. ИПК-4.2. Умеет: анализировать и оценивать угрозы информационной безопасности объекта. ИПК-4.3. Владеет методами проведения анализа рисков информационной безопасности объекта
	06.033 Специалист по защите информации в	D/7 Разработка систем защиты информации автоматизированных систем	D/01.7 Тестирование систем защиты информации автоматизированных систем	ПК-5. Способность проводить анализ, предлагать и обосновывать выбор решений по	ИПК-5.1. Знает: требования к шифрам и основные характеристики шифров;

	автоматизированных системах			обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	архитектуру, принципы функционирования, электронную базу современных компьютеров, вычислительных и телекоммуникационных систем; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; основные информационные технологии, используемые в автоматизированных системах; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные

					комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности. ИПК-5.2. Умеет: анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; проектировать структуру и архитектуру

					программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения. ИПК-5.3. Владеет: навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; методами формирования требований по защите информации; методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем; профессиональной терминологией в области информационной безопасности; навыками анализа

					основных узлов и устройств современных автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем.
	06.033 Специалист по защите информации в автоматизированных системах	D/7 Разработка систем защиты информации автоматизированных систем	D/02.7 Разработка проектных решений по защите информации в автоматизированных системах	ПК-6. Способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	ИПК-6.1. Знает: средства обеспечения безопасности данных; основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации; показатели качества программного обеспечения; методологии и методы проектирования программного обеспечения; методы

					тестирования и отладки ПО; принципы организации документирования разработки, процесса сопровождения программного обеспечения; основные структуры данных и способы их реализации на языке программирования основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности. ИПК-6.2. Умеет: формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; планировать разработку сложного программного обеспечения; проводить комплексное

					тестирование и отладку программных систем; проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач; работать с интегрированной средой разработки программного обеспечения; оценивать информационные риски в автоматизированных системах. ИПК-6.3. Владеет: навыками участия в

					экспертизе состояния защищенности информации на объекте защиты; навыками проектирования программного обеспечения с использованием средств автоматизации; навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; навыками разработки программной документации; навыками программирования с использованием эффективных реализаций структур данных и алгоритмов.
	06.033 Специалист по защите информации в	С/6 Внедрение систем защиты информации	С/01.6 Установка и настройка средств защиты информации	ПК-7. Способность участвовать в разработке	ИПК-7.1. Знает: принципы построения и функционирования,

	автоматизированных системах	автоматизированных систем	в автоматизированных системах	защищенных автоматизированных систем в сфере профессиональной деятельности	примеры реализаций современных систем управления базами данных; архитектуру систем баз данных; основные модели данных; физическую организацию баз данных; последовательность и содержание этапов проектирования баз данных. ИПК-7.2. Умеет: разрабатывать и администрировать базы данных; выделять сущности и связи предметной области; отображать предметную область на конкретную модель данных; нормализовать отношения при проектировании реляционной базы данных; применять требования

					Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации. ИПК-7.3. Владеет: навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации.
Тип задач профессиональной деятельности: контрольно-аналитический					
06 Связь, информационные и коммуникационные технологии (в сфере обеспечения	06.032 Специалист по безопасности компьютерных систем и сетей	С/7 Оценивание уровня безопасности компьютерных систем и сетей	С/01.7 Проведение контрольных проверок работоспособности и эффективности	ПК-8. Способность проводить контрольные проверки работоспособности	ИПК-8.1. Знает: требования к шифрам и основные характеристики шифров;

безопасности информации в автоматизированных системах)			применяемых программно-аппаратных средств защиты информации в компьютерных системах и сетях	применяемых программно-аппаратных, криптографических и технических средств защиты информации	основные информационные технологии, используемые в автоматизированных системах. ИПК-8.2. Умеет: контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем. ИПК-8.3. Владеет: навыками участия в экспертизе состояния защищенности информации на объекте защиты; навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; методами расчета и

					инструментального контроля показателей технической защиты информации; навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков.
	06.032 Специалист по безопасности компьютерных систем и сетей	С/7 Оценивание уровня безопасности компьютерных систем и сетей	С/04.7 Проведение сертификации программно-аппаратных средств защиты информации и анализ результатов	ПК-9. Способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	ИПК-9.1. Знает: требования к шифрам и основные характеристики шифров; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации/ ИПК-9.2. Умеет проводит

					экспериментально-исследовательские работы при сертификации средств защиты информации автоматизированных систем, ИПК-9.3. Владеет навыками проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем.
	06.033 Специалист по защите информации в автоматизированных системах	С/6 Внедрение систем защиты информации автоматизированных систем	С/03.6Анализ уязвимостей внедряемой системы защиты информации	ПК-10. Способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	ИПК-10.1. Знает: возможности технических средств перехвата информации. ИПК-10.2. Умеет проводить экспериментально-исследовательских работы при аттестации автоматизированных систем с учетом нормативных документов по защите информации. ИПК-10.3 Владеет навыками проведения

					экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации.
Тип задач профессиональной деятельности: организационно-управленческий					
06 Связь, информационные и коммуникационные технологии (в сфере обеспечения безопасности информации в автоматизированных системах)	06.033 Специалист по защите информации в автоматизированных системах	D/7 Разработка систем защиты информации автоматизированных систем	D/04.7 Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем	ПК-11. Способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	ИПК-11.1. Знает: основные понятия и методы в области управленческой деятельности; порядок выработки и реализации управленческих решений; содержание управленческой работы руководителя подразделения; проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и

					систем; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. ИПК-11.2. Умеет: оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; проводить мониторинг угроз безопасности компьютерных сетей; контролировать эффективность принятых мер по

					реализации частных политик информационной безопасности автоматизированных систем; администрировать подсистемы информационной безопасности автоматизированных систем. ИПК-11.3. Владеет: навыками обоснования, выбора, реализации и контроля результатов управленческого решения; навыками организации и обеспечения режима секретности; навыками работы с технической документацией на ЭВМ и вычислительные системы.
	06.033 Специалист по защите информации в автоматизированных системах	С/6 Внедрение систем защиты информации автоматизированных систем	С/02.6 Разработка организационно-распорядительных документов по защите информации в	ПК-12. Способность разрабатывать предложения по совершенствованию системы управления информационной	ИПК-12.1. Знает: состав системы управления и требования к ее элементам; основные

			автоматизированных системах	безопасностью автоматизированной системы	криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ. ИПК-12.2. Умеет: эффективно использовать различные методы и средства защиты информации для компьютерных сетей; ИПК-12.3. Владеет методами проведения выбора программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.
	06.033 Специалист по защите	D/7 Разработка систем защиты	D/03.7 Разработка эксплуатационной	ПК-13. Способность разрабатывать	ИПК-13.1. Знает ГОСТы по оформлению

	информации в автоматизированных системах	информации автоматизированных систем	документации на системы защиты информации автоматизированных систем	проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	документов по разработке и регламентированию по обеспечению информационной безопасности. ИПК-13.2. Умеет: разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем. ИПК-13.3. Владеет: навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей,

					программных систем с учетом требований по обеспечению информационной безопасности.
	06.032 Специалист по безопасности компьютерных систем и сетей	С/7 Оценивание уровня безопасности компьютерных систем и сетей	С/02.7 Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей	ПК-14. Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	ИПК-14.1. Знает: основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах. ИПК-14.2. Умеет: эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; контролировать эффективность принятых мер по реализации частных политик информационной

					безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем. ИПК-14.3. Владеет: криптографической терминологией; навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.
	06.033 Специалист по защите информации в	С/6 Внедрение систем защиты информации	С/04.6Внедрение организационных мер по защите информации в	ПК-15. Способность формировать комплекс мер (правила,	ИПК-15.1. Знает: основные задачи и понятия криптографии; требования к шифрам и

	автоматизированных системах	автоматизированных систем	автоматизированных системах	процедуры, методы) для защиты информации ограниченного доступа	основные характеристики шифров; типовые поточные и блочные шифры. ИПК-15.2. Умеет: определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем. ИПК-15.3. Владеет методами формирования комплекса мер по защите информации и ограниченного доступа

	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-16. Способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	ИПК-16.1. Знает: основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации; основные методы управления информационной безопасностью. ИПК-16.2. Умеет: восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем.

					ИПК-16.3. Владеет: навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности; навыками организации и обеспечения режима секретности; навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; навыками использования программно-аппаратных средств обеспечения

					информационной безопасности автоматизированных систем.
	06.033 Специалист по защите информации в автоматизированных системах	B/6 Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	B/04.6 Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций	ПК-17. Способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	ИПК-17.1. Знает: основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ; основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации. ИПК-17.2. Умеет: использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;

					оценивать эффективность и надежность защиты операционных систем; планировать политику безопасности операционных систем эффективно использовать различные методы и средства защиты информации для компьютерных сетей; применять средства обеспечения безопасности данных; проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы. ИПК-17.3. Владеет:

					навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ; методами формирования требований по защите информации; методами управления информационной безопасностью автоматизированных систем; навыками выбора и обоснования критериев

					эффективности функционирования защищенных автоматизированных информационных систем.
	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 B/02.6 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	ПК-18. Способность администрировать подсистему информационной безопасности автоматизированной системы	ИПК-18.1. Знает: типовые шифры с открытыми ключами; технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования; источники и классификацию угроз информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; основные угрозы безопасности информации и модели

					нарушителя в автоматизированных системах; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;

					современные технологии и методы программирования. ИПК-18.2. Умеет: планировать политику безопасности операционных систем; применять средства обеспечения безопасности данных; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; администрировать подсистемы информационной безопасности автоматизированных систем. ИПК-18.3. Владеет: навыками работы с операционными системами семейства Windows и Unix, восстановления операционных систем после сбоев; навыками установки и настройки

					операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности; навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ; навыками работы с технической документацией на ЭВМ и вычислительные

					системы; профессиональной терминологией в области информационной безопасности; навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации; навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы; навыками разработки программной документации.
	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	ПК-19. Способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности	ИПК-19.1. Знает типовые шифры с открытыми ключами. ИПК-19.2. Умеет реализовывать политику безопасности баз данных.

			автоматизированных системах B/06.6 Аудит защищенности информации в автоматизированных системах	автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	ИПК-19.3. Владеет навыками использования типовых криптографических алгоритмов и навыками использования ЭВМ в анализе простейших шифров.
	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	ПК-20. Способность управлять информационной безопасностью автоматизированной системы	ИПК-20.1. Знает основные методы управления информационной безопасностью. ИПК-20.2. Умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем. ИПК-20.3. Владеет методами управления информационной безопасностью автоматизированных систем.

Профессиональные компетенции, установленные программой специалитета, 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 специалитета, обеспечивает выпускнику способность осуществлять профессиональную деятельность не менее чем в одной области профессиональной деятельности и сфере профессиональной деятельности.

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

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).

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 подготовки к процедуре защиты и защиты выпускной квалификационной работы.

VIII. Условия реализации программы специалитета

1. Выполнение общесистемных требований к реализации программы

Университет располагает на законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных 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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» с применением электронного обучения, дистанционных образовательных технологий ЭИОС Университета дополнительно обеспечивает:

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

– 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.

Для реализации программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем в Университете существует специальная кафедра «Информационная безопасность».

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

Помещения для реализации программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» представляют собой учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения, состав которых определен в рабочих программах дисциплин (модулей).

Для реализации программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» в Университете предусмотрены:

1. лаборатории в области:

– физики, оснащенную учебно-лабораторными стендами по механике, электричеству и магнетизму, оптике;

– электроники и схемотехники, оснащенную учебно-лабораторными стендами для изучения работы компонентов узлов и блоков вычислительных устройств, рабочих мест разработчиков систем и устройств в системах автоматизированного проектирования, средствами для измерения и визуализации частотных и временных характеристик сигналов, средствами для измерения параметров электрических цепей, средствами генерирования сигналов;

– сетей и систем передачи информации, оснащенную рабочими местами на базе вычислительной техники, стендами сетей передачи информации с коммутацией пакетов и коммутацией каналов;

– безопасности вычислительных сетей, оснащенную стендами для изучения проводных и беспроводных компьютерных сетей, включающих абонентские устройства, коммутаторы, маршрутизаторы, точки доступа, межсетевые экраны, средства обнаружения компьютерных атак, системы углубленной проверки сетевых пакетов и системы защиты от утечки данных, анализаторы кабельных сетей;

– технической защиты информации, оснащенную специализированным оборудованием по защите информации от утечки по техническим каналам, техническими средствами контроля эффективности защиты информации от утечки по техническим каналам;

– программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, средствами анализа защищенности компьютерных сетей, устройствами чтения смарт-карт и радиометок, программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации;

– автоматизированных систем в защищенном исполнении, оснащенную аппаратно-программными средствами управления доступом к данным, средствами криптографической защиты информации, средствами дублирования и восстановления данных, средствами мониторинга состояния автоматизированных систем, средствами контроля и управления доступом в помещения;

2. специально оборудованные кабинеты (классы, аудитории):

– информационных технологий, оснащенный рабочими местами на базе вычислительной техники и абонентскими устройствами, подключенными к сети «Интернет» с использованием проводных и/или беспроводных технологий;

– научно-исследовательской работы обучающихся, курсового и дипломного проектирования, оснащенный рабочими местами на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и (или) программных средств, а также комплектом оборудования для печати;

– аудитории (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация

ограниченного доступа, не содержащая сведений, составляющих государственную тайну;

– специальная библиотека (библиотеку литературы ограниченного доступа), предназначенную для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа.

Компьютерные (специализированные) классы и лаборатории, в которых предусмотрены рабочие места на базе вычислительной техники, оборудованы современной вычислительной техникой из расчета одно рабочее место на каждого обучающегося при проведении занятий в данных классах (лабораториях).

Университет имеет лаборатории (специально оборудованные кабинеты (классы, аудитории), обеспечивающие практическую подготовку выпускников в соответствии программой специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем».

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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» представлена в Приложении 6.

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

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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных 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).

Не менее 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).

Не менее 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 не менее 65 процентов от общего количества лиц, привлекаемых к реализации программы специалитета.

Не менее 55 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).

В реализации программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» принимает участие

минимум один педагогический работник Университета, имеющий ученую степень или ученое звание по научной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» или по научной специальности, соответствующей направлениям подготовки кадров высшей квалификации по программам подготовки научно-педагогических кадров в адъюнктуре, входящим в укрупненную группу специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

Сведения о кадровом обеспечении программы представлены в Приложении 7.

4. Выполнение требований к финансовым условиям реализации программы

Финансовое обеспечение реализации программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» осуществляется в объеме не ниже значений базовых нормативов затрат на оказание государственных услуг по реализации образовательных программ высшего образования - программ специалитета 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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» определяется в рамках системы внутренней оценки, а также системы внешней оценки, в которой Университет принимает участие на добровольной основе.

В целях совершенствования программы специалитета Университет при проведении регулярной внутренней оценки качества образовательной деятельности и подготовки обучающихся по программе специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» привлекает работодателей и (или) их объединения, иных юридических и (или) физических лиц, включая педагогических работников Университета.

В рамках внутренней системы оценки качества образовательной деятельности по программе специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных 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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» в рамках процедуры государственной аккредитации осуществляется с целью подтверждения соответствия образовательной деятельности по программе специалитета требованиям ФГОС ВО.

Внешняя оценка качества образовательной деятельности и подготовки обучающихся по программе специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных 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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных 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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных 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 специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных 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.