МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

ПРИНЯТО
на заседании
Учёного совета университета
протокол от 19.08.2026 № 7

УТВЕРЖДАЮ
Директор департамента по УР
_____ Ким М.Ю.
19.08.2026

ОСНОВНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ

- программа бакалавриата

Направление подготовки:	10.03.01 Информационная безопасность
Направленность (профиль):	Безопасность компьютерных систем
Квалификация:	бакалавр
Формы обучения:	очная
Факультеты:	Факультет безопасности (ФБ)
Кафедра:	Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ким М.Ю.
Должность: Директор департамента по УР
Дата подписания: 19.08.2026
Уникальный программный ключ:
ed789cd8-2cc6-4431-a59e-8f386b1d44fa

Согласована на портале № 1529

Томск

СОДЕРЖАНИЕ

Раздел 1. ОБЩИЕ ПОЛОЖЕНИЯ 4

1.1. Назначение основной профессиональной образовательной программы 4

1.2. Нормативные документы 4

1.3. Перечень сокращений 5

Раздел 2. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКОВ 6

2.1. Общее описание профессиональной деятельности выпускников 6

2.2. Перечень профессиональных стандартов, соотнесенных с ФГОС ВО 6

2.3. Перечень основных задач профессиональной деятельности выпускников 18

2.4. Ключевые партнеры основной профессиональной образовательной программы 21

Раздел 3. ОБЩАЯ ХАРАКТЕРИСТИКА ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 23

3.1. Цель основной профессиональной образовательной программы 23

3.2. Направленность (профиль) основной профессиональной образовательной программы 23

3.3. Квалификация, присваиваемая выпускникам основной профессиональной образовательной программы 23

3.4. Объем основной профессиональной образовательной программы 24

3.5. Формы обучения 24

3.6. Срок получения образования 24

3.7. Язык реализации основной профессиональной образовательной программы 24

3.8. Использование сетевой формы реализации основной профессиональной образовательной программы 24

3.9. Применение электронного обучения, дистанционных образовательных технологий 24

3.10. Требования к поступающим на основную профессиональную образовательную программу 24

Раздел 4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 26

4.1. Универсальные компетенции выпускников и индикаторы их достижения 26

4.2. Общепрофессиональные компетенции выпускников и индикаторы их достижения 30

4.3. Профессиональные компетенции выпускников и индикаторы их достижения 37

Раздел 5. СТРУКТУРА И СОДЕРЖАНИЕ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 48

5.1. Учебный план 48

5.2. Календарный учебный график 48

Согласована на портале № 1529

5.3. Рабочие программы дисциплин (модулей) 48
5.4. Рабочие программы практик 49
5.5. Оценочные материалы для текущей и промежуточной аттестации по дисциплинам (модулям) и практикам 49
5.6. Рабочая программа государственной итоговой аттестации 49
5.7. Рабочая программа воспитания и календарный план воспитательной работы 50
Раздел 6. УСЛОВИЯ РЕАЛИЗАЦИИ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 52
6.1. Общесистемные требования к реализации основной профессиональной образовательной программы 52
6.2. Требования к материально-техническому и учебно-методическому обеспечению основной профессиональной образовательной программы 53
6.3. Требования к кадровым условиям реализации основной профессиональной образовательной программы 54
6.4. Требования к финансовым условиям реализации основной профессиональной образовательной программы 55
6.5. Требования к применяемым механизмам оценки качества образовательной деятельности и подготовки обучающихся по основной профессиональной образовательной программе 55
6.6. Условия реализации основной профессиональной образовательной программы для инвалидов и лиц с ограниченными возможностями здоровья 56
Раздел 7. РЕЦЕНЗИИ НА ОСНОВНУЮ ПРОФЕССИОНАЛЬНУЮ ОБРАЗОВАТЕЛЬНУЮ ПРОГРАММУ 58
Лист согласования 63

Согласована на портале № 1529

Раздел 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение основной профессиональной образовательной программы

Основная профессиональная образовательная программа по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» реализуемая федеральным государственным автономным образовательным учреждением высшего образования «Томский государственный университет систем управления и радиоэлектроники», является комплексом основных характеристик образования (объем, содержание, планируемые результаты) и организационно-педагогических условий, который представлен в виде учебного плана, календарного учебного графика, рабочих программ дисциплин (модулей), иных компонентов, оценочных и методических материалов, а также, в виде рабочей программы воспитания, календарного плана воспитательной работы, форм аттестации.

Основная профессиональная образовательная программа по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» разработана на основе соответствующего федерального государственного образовательного стандарта высшего образования, с учетом профессиональных стандартов, соответствующих профессиональной деятельности выпускников.

Информация об основной профессиональной образовательной программе по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» размещена на официальном сайте ТУСУРа в сети «Интернет» по адресу https://edu.tusur.ru/opops/1529.

Основная профессиональная образовательная программа по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» обновляется в соответствии с требованиями российского рынка труда, состоянием и перспективами развития науки, культуры, экономики, техники, технологий и социальной сферы.

1.2. Нормативные документы

Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 Информационная безопасность (квалификация (степень) «бакалавр»), утвержденный приказом Министерства образования и науки Российской Федерации от 17.11.2020 № 1427 ;

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденный приказом Министерства науки и высшего образования Российской Федерации от 06.04.2021 № 245 ;

Приказ Министерства науки и высшего образования Российской Федерации и Министерства просвещения Российской Федерации от 05.08.2020 № 885/390 «О практической подготовке обучающихся»;

Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры, утвержденный приказом Министерства образования и науки Российской Федерации

Согласована на портале № 1529

от 29.06.2015 № 636 ;

Профессиональный стандарт «06.001 – Программист», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 20.07.2022 № 424н ;

Профессиональный стандарт «06.026 – Системный администратор информационно-коммуникационных систем», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 29.09.2020 № 680н ;

Профессиональный стандарт «06.030 – Специалист по защите информации в телекоммуникационных системах и сетях», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 536н ;

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

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

Профессиональный стандарт «06.034 – Специалист по технической защите информации», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 09.08.2022 № 474н ;

Профессиональный стандарт «06.042 – Специалист по большим данным», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 06.07.2020 № 405н ;

Устав ТУСУРа;

Локальные нормативные акты ТУСУРа по основным вопросам организации и осуществления образовательной деятельности.

1.3. Перечень сокращений

ВКР – выпускная квалификационная работа
ГИА – государственная итоговая аттестация
з.е. – зачетная единица (1 з.е. – 36 академических часов; 1 з.е. – 27 астрономических часов)
ОВЗ – ограниченные возможности здоровья
ОМ – оценочные материалы
ОПК – общепрофессиональные компетенции
ОПОП – основная профессиональная образовательная программа
ОТФ – обобщенная трудовая функция
ПК – профессиональные компетенции
ПС – профессиональный стандарт
ТФ – трудовая функция
УК – универсальные компетенции
ФГОС ВО – федеральный государственный образовательный стандарт высшего образования
ФТД – факультативные дисциплины

Согласована на портале № 1529

Раздел 2. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКОВ

2.1. Общее описание профессиональной деятельности выпускников

Области профессиональной деятельности и сферы профессиональной деятельности, в которых выпускники, освоившие основную профессиональную образовательную программу по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем», могут осуществлять профессиональную деятельность:

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

В рамках освоения основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» выпускники готовятся к решению задач профессиональной деятельности следующих типов:

– проектно-технологический (основной тип);
– эксплуатационный;
– организационно-управленческий.

Основными объектами (или областями знания) профессиональной деятельности выпускников, освоивших основную профессиональную образовательную программу по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем», являются:

– объекты информатизации (компьютерные системы и сети, программное обеспечение, информационные ресурсы, криптографические системы) в условиях угроз информационной безопасности;
– процессы управления информационной безопасностью (разработка политик, управление инцидентами, оценка рисков, контроль соответствия нормативно-правовым требованиям);
– технологии обеспечения безопасности (технологии безопасной разработки приложений, управление жизненным циклом ПО, криптографические системы, инструменты анализа защищённости кода и мониторинга инцидентов).

2.2. Перечень профессиональных стандартов, соотнесенных с ФГОС ВО

Перечень профессиональных стандартов, соответствующих профессиональной деятельности выпускников, освоивших основную профессиональную образовательную программу по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем»:

Направление подготовки	Направленность (профиль)	Номер уровня квалификации	Код и наименование профессионального стандарта
10.03.01	Безопасность	6	06.001 - Программист;

Согласована на портале № 1529

Информационная безопасность	компьютерных систем		06.026 - Системный администратор информационно-коммуникационных систем; 06.030 - Специалист по защите информации в телекоммуникационных системах и сетях; 06.032 - Специалист по безопасности компьютерных систем и сетей; 06.033 - Специалист по защите информации в автоматизированных системах; 06.034 - Специалист по технической защите информации; 06.042 - Специалист по большим данным.
		5	06.026 - Системный администратор информационно-коммуникационных систем.

Перечень обобщенных трудовых функций и трудовых функций, соответствующих профессиональной деятельности выпускников основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем»:

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	Код	Наименование	Ур.кв.	Код	Наименование	Ур.кв.
06.042 - Специалист по большим данным	A	Анализ больших данных с использованием существующей в организации методологической и технологической инфраструктуры	6	A/01.6	Выявление, формирование и согласование требований к результатам аналитических работ с применением технологий больших данных	6
				A/02.6	Планирование и организация аналитических работ с использованием технологий больших данных	6
				A/03.6	Подготовка данных для	6

Согласована на портале № 1529

					проведения аналитических работ по исследованию больших данных	
				A/04.6	Проведение аналитического исследования с применением технологий больших данных в соответствии с требованиями заказчика	6
06.034 - Специалист по технической защите информации	B	Проведение работ по установке и техническому обслуживанию защищенных средств обработки информации	6	B/01.6	Проведение работ по установке, настройке, испытаниям и техническому обслуживанию защищенных технических средств обработки информации	6
				B/02.6	Проведение работ по установке, монтажу, наладке, испытаниям и техническому обслуживанию защищенных программных (программно-технических) средств обработки информации	6
	E	Проведение контроля защищенности информации	6	E/01.6	Проведение специальных исследований на побочные электромагнитные излучения и	6

Согласована на портале № 1529

					наводки технических средств обработки информации	
				E/02.6	Проведение контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	6
				E/03.6	Проведение контроля защищенности акустической речевой информации от утечки по техническим каналам	6
				E/04.6	Проведение контроля защищенности информации от несанкционированного доступа	6
06.033 - Специалист по защите информации в автоматизированных системах	B	Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий	6	B/01.6	Диагностика систем защиты информации автоматизированных систем	6
				B/02.6	Администрирование систем защиты информации автоматизированных систем	6
				B/03.6	Управление защитой информации в автоматизированн	6

Согласована на портале № 1529

		значимости, в процессе их эксплуатации			ых системах	
				B/04.6	Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций	6
				B/05.6	Мониторинг защищенности информации в автоматизированных системах	6
				B/06.6	Аудит защищенности информации в автоматизированных системах	6
				B/07.6	Установка и настройка средств защиты информации в автоматизированных системах	6
				B/08.6	Разработка организационно-распорядительных документов по защите информации в автоматизированных системах	6
				B/09.6	Анализ уязвимостей внедряемой системы защиты информации	6
				B/10.6	Внедрение организационных мер по защите	6

Согласована на портале № 1529

					информации в автоматизированных системах	
06.032 - Специалист по безопасности компьютерных систем и сетей	B	Администрирование средств защиты информации в компьютерных системах и сетях	6	B/01.6	Администрирование подсистем защиты информации в операционных системах	6
				B/02.6	Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	6
				B/03.6	Администрирование средств защиты информации прикладного и системного программного обеспечения	6
06.030 - Специалист по защите информации в телекоммуникационных системах и сетях	B	Обеспечение защиты от НД и компьютерных атак сооружений и СССЭ (за исключением сетей связи специального назначения) в процессе их эксплуатации	6	B/01.6	Мониторинг функционирования СССЭ, защищенности от НД и компьютерных атак сооружений и СССЭ	6
				B/02.6	Управление функционированием СССЭ, защищенностью от НД и компьютерных атак сооружений и СССЭ	6
				B/03.6	Управление персоналом,	6

Согласована на портале № 1529

					обслуживающим сооружения и СССЭ, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от НД, средства для поиска признаков компьютерных атак в сетях электросвязи	
06.026 - Системный администратор информационно-коммуникационных систем	C	Обслуживание сетевых устройств информационно-коммуникационной системы	6	C/01.6	Выполнение работ по выявлению и устранению сложных инцидентов, возникающих на сетевых устройствах информационно-коммуникационных систем	6
				C/02.6	Проведение анализа и выявление основных причин сложных проблем, возникающих на сетевых устройствах информационно-коммуникационных систем	6
				C/03.6	Разработка планов резервного копирования,	6

Согласована на портале № 1529

	архивирования и восстановления конфигураций сетевых устройств информационно-коммуникационных систем	
С/05.6	Выполнение обновления программного обеспечения сетевых устройств информационно-коммуникационных систем	6
С/06.6	Прогнозирование влияния внешних и внутренних воздействий на поведение сетевых устройств информационно-коммуникационной системы	6
С/07.6	Прогнозирование потребности в изменении объемов ресурсов, необходимых для обеспечения бесперебойной работы сетевых устройств информационно-коммуникационных систем	6
С/08.6	Планирование и проведение работ по распределению нагрузки между имеющимися ресурсами, снятию нагрузки на	6

Согласована на портале № 1529

					сетевые устройства информационно-коммуникационных систем перед проведением регламентных работ, восстановлению штатной схемы работы в случае сбоев	
				C/09.6	Определение потребностей в приобретении специализированных средств контроля и тестирования сетевых устройств информационно-коммуникационных систем	6
	D	Обслуживание серверных операционных систем информационно-коммуникационной системы	6	D/01.6	Выполнение работ по выявлению и устранению нетипичных инцидентов, возникающих в серверных операционных системах информационно-коммуникационной системы	6
				D/02.6	Проведение анализа и определение основных причин сложных проблем, возникающих на серверах и в серверных	6

Согласована на портале № 1529

	операционных системах	
D/03.6	Выполнение планирования резервного копирования, архивирования и восстановления конфигурации серверов и серверных операционных систем	6
D/04.6	Планирование изменений параметров работы серверов и серверных операционных систем	6
D/05.6	Выполнение обновления программного обеспечения серверных операционных систем	6
D/06.6	Прогнозирование влияния внешних и внутренних воздействий на поведение серверных операционных систем	6
D/07.6	Прогнозирование потребности в изменении объемов необходимых ресурсов для	6

Согласована на портале № 1529

					обеспечения бесперебойной работы серверов и серверных операционных систем	
				D/08.6	Планирование и проведение работ по распределению нагрузки между имеющимися ресурсами, снятию нагрузки на серверы и серверные операционные системы перед проведением регламентных работ, восстановлению штатной схемы работы в случае сбоев	6
				D/09.6	Определение потребностей в приобретении специализированных средств контроля и тестирования серверов и серверных операционных систем	6
06.001 - Программист	D	Разработка требований и проектирование программного обеспечения	6	D/01.6	Анализ возможностей реализации требований к компьютерному программному обеспечению	6

Согласована на портале № 1529

				D/02.6	Разработка технических спецификаций на программные компоненты и их взаимодействие	6
				D/03.6	Проектирование компьютерного программного обеспечения	6
06.026 - Системный администратор информационно-коммуникационных систем	B	Обслуживание информационно-коммуникационной системы	5	B/01.5	Выполнение работ по выявлению и устранению инцидентов в информационно-коммуникационных системах	5
				B/02.5	Обеспечение работы технических и программных средств информационно-коммуникационных систем	5
				B/03.5	Реализация схемы резервного копирования, архивирования и восстановления конфигураций технических и программных средств информационно-коммуникационных систем по утвержденным планам	5
				B/04.5	Внесение изменений в технические и	5

Согласована на портале № 1529

					программные средства информационно-коммуникационных систем по утвержденному плану работ	
				B/05.5	Проведение обновления программного обеспечения технических средств информационно-коммуникационных систем по инструкциям производителей	5
				B/06.5	Диагностика исчерпания типовых ресурсов информационно-коммуникационных систем с использованием прикладных программных средств и средств контроля	5
				B/07.5	Проведение предварительных испытаний при проведении работ с возможными рисками перерывов в предоставлении сервисов информационно-коммуникационных систем	5

2.3. Перечень основных задач профессиональной деятельности выпускников

Согласована на портале № 1529

Перечень основных задач профессиональной деятельности выпускников, освоивших основную профессиональную образовательную программу по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем»:

Область профессиональной деятельности (по Реестру Минтруда)	Типы задач профессиональной деятельности	Задачи профессиональной деятельности	Объекты профессиональной деятельности (или области знаний)
06 - Связь, информационные и коммуникационные технологии	организационно-управленческий	Организация и управление системой информационной безопасности на уровне предприятия, включая разработку политик информационной безопасности, координацию деятельности специалистов, управление процессами аудита и контроля соответствия требованиям законодательства; Управление инцидентами и кризисными ситуациями в области информационной безопасности, включая координацию действий специалистов при реагировании на инциденты, взаимодействие с внешними органами, ведение реестра инцидентов и анализ уроков для повышения устойчивости систем.	Объекты информатизации (компьютерные системы и сети, программное обеспечение, информационные ресурсы, криптографические системы) в условиях угроз информационной безопасности; Процессы управления информационной безопасностью (разработка политик, управление инцидентами, оценка рисков, контроль соответствия нормативно-правовым требованиям); Технологии обеспечения безопасности (технологии безопасной разработки приложений, управление жизненным циклом ПО, криптографические системы, инструменты анализа защищённости кода и мониторинга

Согласована на портале № 1529

			инцидентов).
	проектно-технологический	Проектирование архитектуры защищённых информационных систем, включая выбор и интеграцию компонентов системы защиты, разработку политик безопасности, построение схем криптографической защиты данных в соответствии с требованиями нормативной базы; Разработка защищённого программного обеспечения с применением практик безопасного кодирования, SAST/DAST-анализа и управления уязвимостями кода; Проведение оценки рисков информационной безопасности, анализа угроз и уязвимостей, разработка и согласование технических мер по защите информации, создание документации по обеспечению безопасности информационных систем; Управление жизненным циклом защищённого ПО,	Объекты информатизации (компьютерные системы и сети, программное обеспечение, информационные ресурсы, криптографические системы) в условиях угроз информационной безопасности; Процессы управления информационной безопасностью (разработка политик, управление инцидентами, оценка рисков, контроль соответствия нормативно-правовым требованиям); Технологии обеспечения безопасности (технологии безопасной разработки приложений, управление жизненным циклом ПО, криптографические системы, инструменты анализа защищённости кода и мониторинга инцидентов).

Согласована на портале № 1529

		интеграция механизмов безопасности в конвейеры DevOps (CI/CD), автоматизация контроля защищённости.	
	эксплуатационный	Администрирование защищённых компьютерных систем и сетей, включая установку, настройку, мониторинг и техническое обслуживание средств защиты; Оперативный анализ и ответ на инциденты информационной безопасности, включая выявление признаков компьютерных атак, сбор свидетельств, реагирование на инциденты, восстановление после происшествий и документирование результатов анализа.	Объекты информатизации (компьютерные системы и сети, программное обеспечение, информационные ресурсы, криптографические системы) в условиях угроз информационной безопасности; Процессы управления информационной безопасностью (разработка политик, управление инцидентами, оценка рисков, контроль соответствия нормативно-правовым требованиям); Технологии обеспечения безопасности (технологии безопасной разработки приложений, управление жизненным циклом ПО, криптографические системы, инструменты анализа защищённости кода и мониторинга

Согласована на портале № 1529

			инцидентов).

2.4. Ключевые партнеры основной профессиональной образовательной программы

Ключевыми партнерами, участвующими в формировании и реализации основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем», являются:

- АО "Аладдин Р.Д.", г. Москва, Россия;
- АО "ИнфоТеКС", г. Москва, Россия;
- ООО "Юзергейт", г. Новосибирск, Новосибирская область, Россия.

Согласована на портале № 1529

Раздел 3. ОБЩАЯ ХАРАКТЕРИСТИКА ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

3.1. Цель основной профессиональной образовательной программы

Основная профессиональная образовательная программа по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» имеет своей целью формирование у обучающихся совокупности универсальных, общепрофессиональных и профессиональных компетенций, которая должна обеспечивать выпускнику способность осуществлять профессиональную деятельность не менее чем в одной области профессиональной деятельности и сфере профессиональной деятельности, установленных ФГОС ВО, и решать задачи профессиональной деятельности не менее чем одного типа, установленного ФГОС ВО.

В области воспитания целью ОПОП является создание условий для активной жизнедеятельности обучающихся, их гражданского самоопределения, профессионального становления и индивидуально-личностной самореализации в созидательной деятельности для удовлетворения потребностей в нравственном, культурном, интеллектуальном, социальном и профессиональном развитии.

Основная профессиональная образовательная программа по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем»:

– подготавливает компетентных специалистов в области информационной безопасности, способных осуществлять полный цикл профессиональной деятельности: проектирование, разработку, внедрение, эксплуатацию и сопровождение защищённых компьютерных систем, криптографических механизмов и средств защиты информации, обеспечивая защиту информационных активов организаций;

– способствует формированию у выпускников способности обеспечивать киберустойчивость критически важных объектов информационной инфраструктуры в реализацию государственной политики информационной безопасности, в соответствии с Доктриной информационной безопасности Российской Федерации, Указом Президента РФ от 01.05.2022 № 250 и национальным проектом «Экономика данных и цифровая трансформация государства»;

– осуществляет подготовку специалистов в области безопасной разработки приложений, владеющих компетенциями в применении методологии DevSecOps, анализа защищённости кода (SAST/DASTметоды) и управления уязвимостями, способных интегрировать механизмы безопасности на всех этапах жизненного цикла программного обеспечения, обеспечивая технологический суверенитет и конкурентоспособность российских информационных систем.

3.2. Направленность (профиль) основной профессиональной образовательной программы

Основная профессиональная образовательная программа по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем».

3.3. Квалификация, присваиваемая выпускникам основной профессиональной образовательной программы

Выпускникам, освоившим основную профессиональную образовательную программу по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля)

Согласована на портале № 1529

«Безопасность компьютерных систем», присваивается квалификация «бакалавр».

3.4. Объем основной профессиональной образовательной программы

Объем основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» составляет 240 з.е. вне зависимости от формы обучения, применяемых образовательных технологий, реализации основной профессиональной образовательной программы с использованием сетевой формы, реализации основной профессиональной образовательной программы по индивидуальному учебному плану.

3.5. Формы обучения

Обучение по основной профессиональной образовательной программе по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» осуществляется в очной форме.

3.6. Срок получения образования

Срок получения образования по основной профессиональной образовательной программе по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем», включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, вне зависимости от применяемых образовательных технологий, составляет:

Форма обучения	Срок получения образования
очная	4 года

3.7. Язык реализации основной профессиональной образовательной программы

Основная профессиональная образовательная программа по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» реализуется на государственном языке Российской Федерации.

3.8. Использование сетевой формы реализации основной профессиональной образовательной программы

Основная профессиональная образовательная программа по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» реализуется без использования сетевой формы.

3.9. Применение электронного обучения, дистанционных образовательных технологий

Основная профессиональная образовательная программа по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» реализуется с применением электронного обучения, дистанционных образовательных технологий.

3.10. Требования к поступающим на основную профессиональную образовательную программу

К освоению основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность

Согласована на портале № 1529

компьютерных систем» допускаются лица, имеющие среднее общее образование.

Согласована на портале № 1529

Раздел 4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4.1. Универсальные компетенции выпускников и индикаторы их достижения

В результате освоения основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» у выпускника должны быть сформированы все универсальные компетенции:

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
Системное и критическое мышление	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 - Знает методики сбора и обработки информации, актуальные российские и зарубежные источники информации для решения поставленных задач, а также методы системного анализа; УК-1.2 - Умеет применять методики поиска, сбора и обработки информации, осуществлять критический анализ и синтез информации, полученной из разных источников; УК-1.3 - Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации, методикой системного подхода для решения поставленных задач; способен генерировать различные варианты решения поставленных задач.
Разработка и реализация проектов	УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 - Знает виды ресурсов и ограничений для решения поставленных задач, основные методы оценки разных способов решения задач, действующее законодательство и правовые нормы, регулирующие профессиональную деятельность; УК-2.2 - Умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения, анализировать альтернативные варианты решений для достижения намеченных результатов, использовать нормативно-правовую документацию в сфере профессиональной деятельности; находит оптимальные способы решения поставленных

Согласована на портале № 1529

		задач; УК-2.3 - Владеет методиками постановки цели и задач проекта, методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией; проводит рефлексию и оценку результатов проекта.
Командная работа и лидерство	УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3.1 - Знает основные приемы и нормы социального взаимодействия, основные понятия и методы конфликтологии, технологии межличностной и групповой коммуникации в деловом взаимодействии; УК-3.2 - Умеет устанавливать и поддерживать контакты, обеспечивающие успешную работу в коллективе, применять основные методы и нормы социального взаимодействия для реализации своей роли и взаимодействия внутри команды; УК-3.3 - Владеет основными методами и приемами социального взаимодействия и работы в команде; учитывает мнения и особенности поведения окружающих; ориентирован на результат.
Коммуникация	УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	УК-4.1 - Знает принципы построения устного и письменного высказывания на русском и иностранном(ых) языках, правила и закономерности деловой устной и письменной коммуникации; владеет широким словарным запасом, достаточным для осуществления деловой коммуникации в рамках академической и профессиональной направленности; УК-4.2 - Имеет представление об особенностях устной и письменной коммуникации в соответствии с различными стилями, жанрами и формами делового общения; выбирает коммуникативно приемлемые стили делового общения, вербальные и невербальные средства коммуникации; УК-4.3 - Умеет составлять собственные устные и письменные высказывания на русском и иностранном(ых) языках в

Согласована на портале № 1529

		соответствии с речевыми ситуациями, наиболее востребованными в рамках академической и профессиональной направленности; УК-4.4 - Владеет навыками применения информационно-коммуникационных технологий для осуществления деловой коммуникации на русском и иностранном(ых) языке(ах) в письменной и устной форме.
Межкультурное взаимодействие	УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	УК-5.1 - Знает особенности социально-исторического развития различных культур, особенности межкультурного разнообразия общества, правила и технологии эффективного межкультурного взаимодействия; УК-5.2 - Умеет понимать и воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах; УК-5.3 - Владеет навыками общения в мире культурного многообразия с использованием этических норм поведения.
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	УК-6.1 - Знает основные приемы и принципы эффективного управления собственным временем, основные методики самоконтроля, саморазвития и самообучения; принципы непрерывного образования / принципы образования в течение всей жизни; УК-6.2 - Умеет эффективно планировать и контролировать собственное время, использовать современные методы и цифровые инструменты тайм-менеджмента для повышения личной эффективности в процессе обучения и профессионального развития; УК-6.3 - Владеет навыками самодиагностики и рефлексии для корректировки траектории саморазвития и повышения эффективности достижения поставленных перед собой целей и задач; понимает значимость образования в течение всей жизни.
	УК-7. Способен	УК-7.1 - Знает виды физических упражнений,

Согласована на портале № 1529

	поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	роль и значение физической культуры в жизни человека и общества в целом, научно-практические основы физической культуры; УК-7.2 - Умеет применять на практике разнообразные средства физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей жизни и профессиональной деятельности; УК-7.3 - Владеет средствами и методами укрепления индивидуального здоровья для обеспечения полноценной социальной и профессиональной деятельности.
Безопасность жизнедеятельности	УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.1 - Знает классификацию и источники чрезвычайных ситуаций природного и техногенного происхождения, причины, признаки и последствия опасностей, способы защиты от чрезвычайных ситуаций, а также принципы организации безопасности труда на предприятии, технические средства защиты людей в условиях чрезвычайной ситуации; УК-8.2 - Умеет создавать и поддерживать безопасные условия жизнедеятельности, выявлять признаки, причины и условия возникновения чрезвычайных ситуаций, а также оценивать вероятность возникновения потенциальной опасности и принимать меры по ее предупреждению; УК-8.3 - Умеет применять в практической деятельности требования законодательства в области охраны труда, направленные на обеспечение безопасности персонала и населения, в том числе в условиях возникновения чрезвычайных ситуаций природного и техногенного характера; УК-8.4 - Владеет навыками по применению основных методов защиты при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.
Экономическая культура, в том числе финансовая грамотность	УК-9. Способен принимать обоснованные экономические решения в различных областях	УК-9.1 - Знает базовые принципы функционирования экономики и экономического развития общества, источники финансирования

	жизнедеятельности	профессиональной деятельности, критерии оценки затрат и обоснованности экономических решений; УК-9.2 - Умеет принимать и обосновывать экономические решения в различных областях жизнедеятельности, планировать деятельность с учетом экономически оправданных затрат, направленных на достижение результата; УК-9.3 - Владеет основами финансовой грамотности, а также навыками расчета и оценки экономической целесообразности планируемой деятельности (проекта), ее (его) финансирования из различных источников.
Гражданская позиция	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-10.1 - Знать нормативное определение коррупции, экстремизма, терроризма; виды коррупционного, экстремистского, террористического поведения, правовые последствия таких видов поведения; УК-10.2 - Умеет взаимодействовать с другими людьми на принципах уважения личности, иных взглядов и культур, распознавать проявления экстремизма; идентифицировать коррупционные действия и сопоставлять их с законодательно установленным наказанием, разъяснять и предостерегать окружающих от коррупционного поведения; действовать в соответствии с инструкциями и правилами поведения во время терроризма; УК-10.3 - Владеет навыками по формированию нетерпимого отношения к проявлениям экстремизма в коллективе, по профилактике и противодействию проявлениям экстремизма в профессиональной среде; навыками по предотвращению и пресечению коррупционного поведения в профессиональной деятельности; навыками выполнения действий по самосохранению и обеспечению безопасности окружающих во время терроризма.

4.2. Общепрофессиональные компетенции выпускников и индикаторы их достижения

В результате освоения основной профессиональной образовательной программы по

Согласована на портале № 1529

направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» у выпускника должны быть сформированы все общепрофессиональные компетенции:

Наименование категории (группы) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
Без группы	ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1 - Знает понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; ОПК-1.2 - Умеет проводить анализ и выбор средств и способов обеспечения информационной безопасности; ОПК-1.3 - Владеет практическими навыками поиска необходимой информации и обеспечения информационной безопасности при решении задач в области профессиональной деятельности.
	ОПК-1.1. Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	ОПК-1.1.1 - Знает основные модели управления доступом (дискреционная, мандатная, ролевая, атрибутная), принципы построения и архитектуру подсистем управления доступом в современных операционных системах, системах управления базами данных и прикладном программном обеспечении; ОПК-1.1.2 - Знает механизмы идентификации и аутентификации пользователей, включая многофакторную аутентификацию, а также принципы их интеграции с подсистемами управления доступом; ОПК-1.1.3 - Умеет разрабатывать политику управления доступом для информационной системы с учётом модели угроз, модели нарушителя и требований нормативных документов, а также настраивать механизмы управления доступом в типовых операционных системах, системах управления базами данных и прикладном программном обеспечении в соответствии с разработанной

Согласована на портале № 1529

		политикой; ОПК-1.1.4 - Умеет проводить контроль корректности реализации политики управления доступом и выявлять отклонения от заданной политики безопасности.
	ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1 - Знает классификацию компьютерных систем, виды информационного взаимодействия и обслуживания, основы построения информационно-вычислительных систем; ОПК-2.2 - Умеет проводить анализ и выбор информационных технологий, программных средств системного и прикладного назначения для решения задач профессиональной деятельности; ОПК-2.3 - Владеет навыками использования информационно-коммуникационных технологий и программных средств системного и прикладного назначения для решения задач профессиональной деятельности.
	ОПК-1.2. Способен администрировать средства защиты информации в компьютерных системах и сетях	ОПК-1.2.1 - Администрирует подсистемы защиты информации в операционных системах; ОПК-1.2.2 - Администрирует программно-аппаратные средства защиты информации в компьютерных сетях; ОПК-1.2.3 - Администрирование средств защиты информации прикладного и системного программного обеспечения.
	ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.1 - Знает основные понятия математического анализа и алгебры, необходимые для решения задач профессиональной деятельности; ОПК-3.2 - Умеет применять основные математические методы, а также методы теории вероятностей и математической статистики для решения задач профессиональной деятельности; ОПК-3.3 - Владеет практическими навыками решения математических задач и построения статистических моделей экспериментов при решении прикладных задач в области

Согласована на портале № 1529

		профессиональной деятельности.
	ОПК-1.3. Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	ОПК-1.3.1 - Знает основные угрозы безопасности информации, обрабатываемой в системах управления базами данных, и встроенные механизмы защиты информации современных СУБД, включая средства управления доступом, аудита, шифрования и обеспечения целостности данных; ОПК-1.3.2 - Знает основные угрозы безопасности информации, передаваемой по компьютерным сетям, и типовые механизмы защиты сетевого взаимодействия, включая принципы построения защищённых виртуальных сетей, средства криптографической защиты сетевого трафика, защищённого удалённого доступа и доверенной загрузки; ОПК-1.3.3 - Знает принципы построения и функционирования межсетевых экранов нового поколения, систем обнаружения и предотвращения вторжений, средств сегментации сетевой инфраструктуры; ОПК-1.3.4 - Умеет настраивать встроенные механизмы защиты информации в системах управления базами данных, формировать политики разграничения доступа к данным и проводить аудит обращений к базе данных.
	ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1 - Знает основные физические законы, физическую сущность явлений и процессов; ОПК-4.2 - Умеет использовать математические модели физических явлений и процессов; ОПК-4.3 - Владеет практическими навыками решения типовых прикладных физических задач.
	ОПК-1.4. Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и	ОПК-1.4.1 - Проводит контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации в компьютерных системах и сетях; ОПК-1.4.2 - Проводит анализ безопасности компьютерных систем;

Согласована на портале № 1529

	корпоративными требованиями	ОПК-1.4.3 - Проводит инструментальный мониторинг защищенности компьютерных систем и сетей.
	ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1 - Знает основные виды и порядок применения нормативных и методических документов, а также порядок соблюдения законодательных ограничений в сфере профессиональной деятельности; ОПК-5.2 - Умеет использовать основные методы правовой оценки различных подходов решения задач в сфере профессиональной деятельности; ОПК-5.3 - Владеет навыками разработки текстовой документации в области профессиональной деятельности в соответствии с нормативными требованиями, регламентирующими деятельность по защите информации.
	ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1 - Знает основные положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа; ОПК-6.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности; ОПК-6.3 - Владеет навыками применения технологий, методов и средств защиты информации ограниченного доступа.
	ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-7.1 - Знает основные технологии разработки программных средств для решения задач в области профессиональной деятельности; ОПК-7.2 - Умеет применять языки программирования для решения профессиональных задач; ОПК-7.3 - Владеет навыками выбора и

Согласована на портале № 1529

		разработки алгоритмов при решении типовых задач программирования, а также навыками разработки и тестирования программ по поставленной спецификации.
	ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1 - Знает принципы поиска, обработки, обобщения и представления информации для решения задач профессиональной деятельности; ОПК-8.2 - Умеет работать с источниками информации, базами данных и нормативной документацией при решении профессиональных задач; ОПК-8.3 - Владеет практическими навыками поиска необходимой информации и обеспечения информационной безопасности при решении задач в области профессиональной деятельности.
	ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1 - Знает основные понятия криптографии и криптографические методы защиты информации; ОПК-9.2 - Умеет определять наличие типовых технических каналов утечки информации, а также применять методики расчета и инструментального контроля показателей технической защиты информации на объектах информатизации; ОПК-9.3 - Владеет практическими навыками обоснованного выбора и использования СКЗИ при решении задач профессиональной деятельности.
	ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ОПК-10.1 - Знает принципы формирования политики информационной безопасности автоматизированных систем; ОПК-10.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; ОПК-10.3 - Владеет навыками разработки политики безопасности информации автоматизированных систем.

Согласована на портале № 1529

	на объекте защиты	
	ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.1 - Знает методики обработки и оценки достоверности результатов измерений; ОПК-11.2 - Умеет строить модели экспериментов при решении прикладных задач, оценивать параметры моделей, описывать и вычислять характеристики критериев проверки гипотез, а также проводить эксперименты, обрабатывать и представлять полученные результаты; ОПК-11.3 - Владеет навыками проведения исследований и экспериментов, оформления отчетов при проведении разработок в области функционирования, развития и обеспечения информационной безопасности автоматизированных систем.
	ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1 - Знает номенклатуру и содержание нормативных правовых актов и нормативных методических документов, применяемых при проектировании защищенных автоматизированных систем; ОПК-12.2 - Умеет проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств; ОПК-12.3 - Владеет навыками проектирования элементов защищенных автоматизированных систем и разработки необходимой технической документации в области проектирования защищенных автоматизированных систем с учетом действующих нормативных и методических документов.
	ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для	ОПК-13.1 - Знает периодизацию, основные факты, явления и процессы всемирной и отечественной истории; ОПК-13.2 - Умеет анализировать основные этапы и закономерности исторического развития России, в том числе для формирования гражданской позиции и

Согласована на портале № 1529

	формирования гражданской позиции и развития патриотизма	развития патриотизма; ОПК-13.3 - Владеет навыками проведения анализа социально-политической обстановки в стране и в мире с точки зрения закономерностей исторического развития.

4.3. Профессиональные компетенции выпускников и индикаторы их достижения

В результате освоения основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» у выпускника должны быть сформированы все профессиональные компетенции по типам задач профессиональной деятельности:

Задача профессиональной деятельности	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции	Основание (профессиональный стандарт, анализ 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)
Тип задач профессиональной деятельности: проектно-технологический				
Проектирование архитектуры защищённых	Объекты информатизации	ДСО-1 - Способен проектировать, внедрять и	ДСО-1.1 - Управляет жизненным циклом инфраструктуры с	06.026 - Системный администратор

Согласована на портале № 1529

информационных систем, включая выбор и интеграцию компонентов системы защиты, разработку политик безопасности, построение схем криптографической защиты данных в соответствии с требованиями нормативной базы; Разработка защищённого программного обеспечения с применением практик безопасного кодирования, SAST/DAST-анализа и управления уязвимостями кода; Проведение оценки рисков информационной безопасности, анализа угроз и уязвимостей, разработка и согласование технических мер по защите информации, создание	(компьютерные системы и сети, программное обеспечение, информационные ресурсы, криптографические системы) в условиях угроз информационной безопасности; Процессы управления информационной безопасностью (разработка политик, управление инцидентами, оценка рисков, контроль соответствия нормативно-правовым требованиям); Технологии обеспечения безопасности (технологии безопасной разработки приложений, управление жизненным	поддерживать интегрированные процессы обеспечения информационной безопасности в средах разработки, тестирования и эксплуатации программного обеспечения	учетом требований по обеспечению информационной безопасности; ДСО-1.2 - Умеет обосновывать выбор используемых программно-аппаратных средств защиты; ДСО-1.3 - Владеет навыками управления жизненным циклом безопасной разработки.	информационно-коммуникационных систем; 06.032 - Специалист по безопасности компьютерных систем и сетей.

документации по обеспечению безопасности информационных систем; Управление жизненным циклом защищённого ПО, интеграция механизмов безопасности в конвейеры DevOps (CI/CD), автоматизация контроля защищённости.	циклом ПО, криптографические системы, инструменты анализа защищённости кода и мониторинга инцидентов).			
Проектирование архитектуры защищённых информационных систем, включая выбор и интеграцию компонентов системы защиты, разработку политик безопасности, построение схем криптографической защиты данных в соответствии с требованиями нормативной базы; Разработка защищённого программного обеспечения с	Объекты информатизации (компьютерные системы и сети, программное обеспечение, информационные ресурсы, криптографические системы) в условиях угроз информационной безопасности; Процессы управления информационной безопасностью	КБ-ДРП-1 - Способен обеспечивать защиту разрабатываемых и используемых компанией приложений	КБ-ДРП-1.1 - Внедряет процессы безопасной разработки; КБ-ДРП-1.2 - Использует инструменты безопасной разработки; КБ-ДРП-1.3 - Использует методы конструктивной безопасности при проектировании и разработке.	06.001 - Программист.

применением практик безопасного кодирования, SAST/DAST-анализа и управления уязвимостями кода; Проведение оценки рисков информационной безопасности, анализа угроз и уязвимостей, разработка и согласование технических мер по защите информации, создание документации по обеспечению безопасности информационных систем; Управление жизненным циклом защищённого ПО, интеграция механизмов безопасности в конвейеры DevOps (CI/CD), автоматизация контроля защищённости.	(разработка политик, управление инцидентами, оценка рисков, контроль соответствия нормативно-правовым требованиям); Технологии обеспечения безопасности (технологии безопасной разработки приложений, управление жизненным циклом ПО, криптографические системы, инструменты анализа защищённости кода и мониторинга инцидентов).			
Проектирование архитектуры защищённых информационных систем,	Объекты информатизации (компьютерные системы	КБ-ДРП-2 - Способен обеспечивать безопасность моделей машинного обучения на всех этапах их	КБ-ДРП-2.1 - Внедряет процесс безопасности моделей машинного обучения;	06.001 - Программист; 06.042 - Специалист по большим

Согласована на портале № 1529

включая выбор и интеграцию компонентов системы защиты, разработку политик безопасности, построение схем криптографической защиты данных в соответствии с требованиями нормативной базы; Разработка защищённого программного обеспечения с применением практик безопасного кодирования, SAST/DAST-анализа и управления уязвимостями кода; Проведение оценки рисков информационной безопасности, анализа угроз и уязвимостей, разработка и согласование технических мер по защите информации, создание документации по обеспечению	и сети, программное обеспечение, информационные ресурсы, криптографические системы) в условиях угроз информационной безопасности; Процессы управления информационной безопасностью (разработка политик, управление инцидентами, оценка рисков, контроль соответствия нормативно-правовым требованиям); Технологии обеспечения безопасности (технологии безопасной разработки приложений, управление жизненным циклом ПО, криптографи	жизненного цикла, начиная от разработки и обучения и заканчивая развертыванием и эксплуатацией	КБ-ДРП-2.2 - Умеет анализировать и обеспечивать защищенность системы искусственного интеллекта на всех этапах ее жизненного цикла; КБ-ДРП-2.3 - Умеет проводить валидацию систем искусственного интеллекта, оценивает эффективность и качество обеспечения защищенности и безопасности.	данным.

Согласована на портале № 1529

безопасности информационных систем; Управление жизненным циклом защищённого ПО, интеграция механизмов безопасности в конвейеры DevOps (CI/CD), автоматизация контроля защищённости.	ческие системы, инструменты анализа защищённости кода и мониторинга инцидентов).			
Тип задач профессиональной деятельности: организационно-управленческий				
Организация и управление системой информационной безопасности на уровне предприятия, включая разработку политик информационной безопасности, координацию деятельности специалистов, управление процессами аудита и контроля соответствия требованиям законодательства; Управление	Объекты информатизации (компьютерные системы и сети, программное обеспечение, информационные ресурсы, криптографические системы) в условиях угроз информационной безопасности; Процессы управления информационной безопасностью	УНК-02 - Способен применять методы коллективной работы в профессиональной деятельности	УНК-02.1 - Принимает участие в групповом взаимодействии в ходе профессиональной деятельности; УНК-02.2 - Проявляет лидерство и осуществляет наставничество; УНК-02.3 - Знает методы оценки эффективности работы команды и индивидуальных участников.	06.026 - Системный администратор информационно-коммуникационных систем.

инцидентами и кризисными ситуациями в области информационной безопасности, включая координацию действий специалистов при реагировании на инциденты, взаимодействие с внешними органами, ведение реестра инцидентов и анализ уроков для повышения устойчивости систем.	(разработка политик, управление инцидентами, оценка рисков, контроль соответствия нормативно-правовым требованиям); Технологии обеспечения безопасности (технологии безопасной разработки приложений, управление жизненным циклом ПО, криптографические системы, инструменты анализа защищённости кода и мониторинга инцидентов).			
Организация и управление системой информационной безопасности на уровне предприятия, включая разработку политик информационн	Объекты информатизации (компьютерные системы и сети, программное обеспечение, информационные ресурсы, криптографи	КБ-2 - Способен анализировать, оценивать и коммуницировать риски информационной безопасности в контексте бизнес-целей	КБ-2.1 - Проводит оценку рисков с учетом бизнес-последствий; КБ-2.2 - Обеспечивает соответствие регуляторным требованиям; КБ-2.3 - Коммуницирует риски и стратегии ИБ нетехническим	06.026 - Системный администратор информационно-коммуникационных систем; 06.033 - Специалист по защите информации в автоматизированных системах.

Согласована на портале № 1529

ой безопасности, координацию деятельности специалистов, управление процессами аудита и контроля соответствия требованиям законодательства; Управление инцидентами и кризисными ситуациями в области информационной безопасности, включая координацию действий специалистов при реагировании на инциденты, взаимодействие с внешними органами, ведение реестра инцидентов и анализ уроков для повышения устойчивости систем.	ческие системы) в условиях угроз информационной безопасности; Процессы управления информационной безопасностью (разработка политик, управление инцидентами, оценка рисков, контроль соответствия нормативно-правовым требованиям); Технологии обеспечения безопасности (технологии безопасной разработки приложений, управление жизненным циклом ПО, криптографические системы, инструменты анализа защищённости кода и мониторинга		заинтересованным сторонам.	

	инцидентов).			
Тип задач профессиональной деятельности: эксплуатационный				
Администрирование защищённых компьютерных систем и сетей, включая установку, настройку, мониторинг и техническое обслуживание средств защиты; Оперативный анализ и ответ на инциденты информационной безопасности, включая выявление признаков компьютерных атак, сбор свидетельств, реагирование на инциденты, восстановление после происшествий и документирование результатов анализа.	Объекты информатизации (компьютерные системы и сети, программное обеспечение, информационные ресурсы, криптографические системы) в условиях угроз информационной безопасности; Процессы управления информационной безопасностью (разработка политик, управление инцидентами, оценка рисков, контроль соответствия нормативно-правовым требованиям); Технологии обеспечения безопасности	КБ-ДРП-3 - Способен обеспечивать киберустойчивость информационных систем и непрерывность бизнес-процессов	КБ-ДРП-3.1 - Разрабатывает и актуализирует стратегию обеспечения непрерывности бизнеса и аварийного восстановления в контексте киберугроз; КБ-ДРП-3.2 - Проектирует и внедряет архитектурные решения, повышающие киберустойчивость; КБ-ДРП-3.3 - Умеет оценивать и выбирать технологии с точки зрения их вклада в инфраструктурную киберустойчивость.	06.033 - Специалист по защите информации в автоматизированных системах; 06.032 - Специалист по безопасности компьютерных систем и сетей; 06.026 - Системный администратор информационно-коммуникационных систем.

	(технологии безопасной разработки приложений, управление жизненным циклом ПО, криптографические системы, инструменты анализа защищённости кода и мониторинга инцидентов).			
Администрирование защищённых компьютерных систем и сетей, включая установку, настройку, мониторинг и техническое обслуживание средств защиты; Оперативный анализ и ответ на инциденты информационной безопасности, включая выявление признаков компьютерных атак, сбор свидетельств, реагирование на инциденты, восстановление после	Объекты информатизации (компьютерные системы и сети, программное обеспечение, информационные ресурсы, криптографические системы) в условиях угроз информационной безопасности; Процессы управления информационной безопасностью (разработка политик,	ППК-ОС7 - Способен настраивать и обеспечивать работоспособность систем резервного копирования и восстановления данных	ППК-ОС7.1 - Проектирует стратегии резервного копирования; ППК-ОС7.2 - Настраивает и обслуживает системы резервного копирование; ППК-ОС7.3 - Обеспечивает восстановление данных; ППК-ОС7.4 - Выполняет мониторинг и оптимизацию системы резервного копирования.	06.033 - Специалист по защите информации в автоматизированных системах; 06.026 - Системный администратор информационно-коммуникационных систем.

Согласована на портале № 1529

происшествий и документирование результатов анализа.	управление инцидентами, оценка рисков, контроль соответствия нормативно-правовым требованиям); Технологии обеспечения безопасности (технологии безопасной разработки приложений, управление жизненным циклом ПО, криптографические системы, инструменты анализа защищённости кода и мониторинга инцидентов).			

Раздел 5. СТРУКТУРА И СОДЕРЖАНИЕ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

5.1. Учебный план

Учебный план разработан с учетом требований к структуре и условиям реализации основной профессиональной образовательной программы, сформулированных в разделах II, III, IV ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность.

Учебный план определяет перечень, трудоемкость, последовательность и распределение по периодам обучения дисциплин (модулей), практики, иных видов учебной деятельности, формы промежуточной аттестации обучающихся. В учебном плане выделен объем работы обучающихся во взаимодействии с преподавателем (далее – контактная работа) по видам учебных занятий и самостоятельной работы обучающихся.

При реализации основной профессиональной образовательной программы обучающимся обеспечивается возможность освоения элективных дисциплин (модулей) (избираемых в обязательном порядке) и факультативных дисциплин (модулей) (необязательных для изучения при освоении основной профессиональной образовательной программы). Избранные обучающимся элективные и факультативные дисциплины (модули) являются обязательными для освоения.

Учебные планы основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» для всех реализуемых форм обучения размещены на официальном сайте ТУСУРа в сети «Интернет»:

Форма обучения	Год начала подготовки по учебному плану	Документ
очная	2026	https://edu.tusur.ru/programs/2025

5.2. Календарный учебный график

Календарный учебный график разработан в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность. В графике указана последовательность реализации основной профессиональной образовательной программы по годам, включая теоретическое обучение, практики, промежуточные и итоговую аттестации, каникулы.

Календарные учебные графики основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» включены в состав соответствующих учебных планов и доступны по адресам, указанным в п. 5.1.

5.3. Рабочие программы дисциплин (модулей)

Структура рабочих программ дисциплин (модулей) регламентируется локальным нормативным актом ТУСУРа.

Рабочие программы дисциплин (модулей) основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности

Согласована на портале № 1529

(профиля) «Безопасность компьютерных систем» для всех реализуемых форм обучения размещены на официальном сайте ТУСУРа в сети «Интернет» и доступны по адресам, указанным в п. 5.1.

5.4. Рабочие программы практик

Структура рабочих программ практик регламентируется локальным нормативным актом ТУСУРа.

Рабочие программы практик основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» для всех реализуемых форм обучения размещены на официальном сайте ТУСУРа в сети «Интернет» и доступны по адресам, указанным в п. 5.1.

5.5. Оценочные материалы для текущей и промежуточной аттестации по дисциплинам (модулям) и практикам

Оценочные материалы – это совокупность материалов (заданий, методических материалов для определения процедур, критериев оценок и т.д.) для определения уровня сформированности компетенций обучающихся и выпускников, установленных федеральными государственными стандартами высшего образования и формируемых конкретной основной профессиональной образовательной программой.

Оценочные материалы являются приложением к рабочим программам дисциплин (модулей) и практик и включают в себя:

– перечень типовых контрольных заданий или иных материалов, необходимых для оценки результатов обучения по дисциплине (модулю) или практике (задания для семинаров, практических занятий и лабораторных работ, коллоквиумов, контрольных работ, зачетов и экзаменов, контрольные измерительные материалы для тестирования, примерная тематика курсовых работ, рефератов, докладов и т.п.);

– методические материалы, определяющие процедуры и критерии оценивания результатов обучения по дисциплине (модулю) или практике.

Примерный перечень оценочных материалов основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся: вопросы и задания для проведения экзамена (зачёта); отчёт по практике (дневник практики); кейс-задача; коллоквиум; контрольная работа; разноуровневые задачи и задания; реферат; доклад (сообщение); собеседование; творческое задание; тест и др.

В целях приближения текущего контроля успеваемости и промежуточной аттестации обучающихся к задачам их будущей профессиональной деятельности университет привлекает к экспертизе оценочных материалов представителей работодателей из числа действующих руководителей и работников профильных организаций.

5.6. Рабочая программа государственной итоговой аттестации

Государственная итоговая аттестация является заключительным этапом освоения основной профессиональной образовательной программы. В ходе государственной итоговой аттестации устанавливается уровень подготовки выпускника, освоившего основную профессиональную

Согласована на портале № 1529

образовательную программу по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем», к выполнению профессиональных задач и соответствия его подготовки требованиям стандарта.

Государственная итоговая аттестация по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» включает в себя:

– подготовка к процедуре защиты и защита выпускной квалификационной работы.

Структура рабочей программы государственной итоговой аттестации регламентируется локальным нормативным актом ТУСУРа.

Рабочие программы государственной итоговой аттестации основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» для всех реализуемых форм обучения размещены на официальном сайте ТУСУРа в сети «Интернет» и доступны по адресам, указанным в п. 5.1.

5.7. Рабочая программа воспитания и календарный план воспитательной работы

Цель воспитательной работы – создание условий для активной жизнедеятельности обучающихся, их гражданского самоопределения, профессионального становления и индивидуально-личностной самореализации в созидательной деятельности для удовлетворения потребностей в нравственном, культурном, интеллектуальном, социальном и профессиональном развитии.

Задачи воспитательной работы в ТУСУР:

– развитие мировоззрения и актуализация системы базовых ценностей личности;

– приобщение студенчества к общечеловеческим нормам морали, национальным устоям и академическим традициям;

– воспитание уважения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности;

– воспитание положительного отношения к труду, воспитание социально значимой целеустремленности и ответственности в деловых отношениях;

– обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств, необходимых для эффективной профессиональной деятельности;

– выявление и поддержка талантливой молодежи, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации;

– формирование культуры и этики профессионального общения;

– воспитание внутренней потребности личности в здоровом образе жизни, ответственного отношения к природной и социокультурной среде;

– повышение уровня культуры безопасного поведения;

– развитие личностных качеств и установок, социальных навыков и управленческих способностей.

В основу программы воспитания ТУСУР (https://regulations.tusur.ru/documents/1118) положен комплекс методологических подходов, включающий: аксиологический (ценностно-ориентированный), системный, системно-деятельностный, культурологический, проблемно-функциональный, научно-исследовательский, проектный, ресурсный, здоровьесберегающий и информационный подходы.

Согласована на портале № 1529

Основные направления воспитательной работы в ТУСУР:

– гражданское-патриотическое воспитание;

– социализация и духовно-нравственное воспитание;

– научно-образовательное воспитание, молодежное предпринимательство и проектная деятельность;

– физическое воспитание, спорт и популяризация здорового образа жизни;

– культурно-просветительское воспитание и творческое развитие;

– профессиональное и трудовое воспитание;

– экологическое воспитание;

– социальное партнерство и студенческое самоуправление;

– профилактика социально-негативных явлений в молодежной среде.

Виды деятельности:

– проектная деятельность;

– научно-исследовательская деятельность;

– общественная деятельность и студенческое самоуправление;

– волонтерская (добровольческая) деятельность;

– спортивная и физкультурно-оздоровительная деятельность;

– досуговая, культурно-творческая деятельность;

– профориентационная деятельность;

– проведение значимых событий и мероприятий;

– вовлечение обучающихся в предпринимательскую деятельность.

Рабочие программы воспитания и календарные планы воспитательной работы основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» для всех реализуемых форм обучения размещены на официальном сайте ТУСУРа в сети «Интернет» и доступны по адресам, указанным в п. 5.1.

Согласована на портале № 1529

Раздел 6. УСЛОВИЯ РЕАЛИЗАЦИИ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Требования к условиям реализации основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» включают в себя общесистемные требования, требования к материально-техническому и учебно-методическому обеспечению, требования к кадровым и финансовым условиям реализации основной профессиональной образовательной программы, а также требования к применяемым механизмам оценки качества образовательной деятельности и подготовки обучающихся по основной профессиональной образовательной программе.

6.1. Общесистемные требования к реализации основной профессиональной образовательной программы

Университет располагает материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» по Блоку 1 «Дисциплины (модули)» и Блоку 3 «Государственная итоговая аттестация» в соответствии с учебным планом, которое закреплено учредителем за университетом на правах оперативного управления.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» как на территории ТУСУРа, так и вне ее. Условия для функционирования электронной информационно-образовательной среды созданы с использованием собственных ресурсов и ресурсов иных организаций:

– официальный сайт ТУСУРа https://tusur.ru;
– научно-образовательный портал ТУСУРа https://edu.tusur.ru;
– электронная система дистанционного обучения ТУСУРа https://sdo.tusur.ru;
– электронно-библиотечные системы https://lib.tusur.ru.

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), практик;

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

При реализации основной профессиональной образовательной программы с применением электронного обучения, дистанционных образовательных технологий электронная информационно-образовательная среда университета дополнительно обеспечивает:

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

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

Согласована на портале № 1529

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

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

При реализации программы бакалавриата в ТУСУРе создана отдельная кафедра КИБЭВС на факультете безопасности, деятельность которой направлена на реализацию образовательных программ высшего образования по специальностям и направлениям подготовки, входящим в укрупненную группу специальностей и направлений подготовки 10.00.00 "Информационная безопасность".

6.2. Требования к материально-техническому и учебно-методическому обеспечению основной профессиональной образовательной программы

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных основной профессиональной образовательной программой по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем», оснащенные оборудованием и техническими средствами обучения, состав которых определен в рабочих программах дисциплин (модулей).

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

Допускается замена оборудования его виртуальными аналогами.

Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства (состав определен в рабочих программах дисциплин (модулей) и обновляется при необходимости).

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

Минимально необходимый для реализации программы бакалавриата перечень материально-технического обеспечения включает в себя специально оборудованные помещения для проведения учебных занятий, в том числе: лаборатории: - физики, оснащенную учебно-лабораторными стендами по механике, электричеству и магнетизму, оптике; - электротехники, электроники и схемотехники, оснащенные учебно-лабораторными стендами и контрольно-измерительной аппаратурой для измерения частотных свойств, форм и временных характеристик сигналов, средствами для

Согласована на портале № 1529

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, структурированной кабельной системой, стойками с телекоммуникационным оборудованием, системой питания и вентиляции, эмулятором (эмуляторами) активного сетевого оборудования, специализированным программным обеспечением для настройки телекоммуникационного оборудования; - технической защиты информации, оснащенную техническими средствами контроля эффективности защиты информации от утечки по указанным каналам; - программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации (средствами анализа защищенности компьютерных сетей, аппаратно-программными средствами управления доступом к данным, стендами для изучения проводных и беспроводных компьютерных сетей, включающими абонентские устройства, коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, средства обнаружения компьютерных атак; специально оборудованные кабинеты (классы, аудитории): - информатики, технологий и методов программирования, оснащенный рабочими местами на базе вычислительной техники, подключенными к локальной вычислительной сети и сети "Интернет", сетевым программным обеспечением, обучающим программным обеспечением; - защищенного документооборота, оснащенный рабочими местами на базе офисной техники, обучающими стендами и материалами; аудиторию (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну; специальную библиотеку (библиотеку литературы ограниченного доступа), предназначенную для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа. Компьютерные (специализированные) классы и лаборатории, если в них предусмотрены рабочие места на базе вычислительной техники, оборудованы современной вычислительной техникой из расчета одно рабочее место на каждого обучаемого при проведении занятий в данных классах (лабораториях).

6.3. Требования к кадровым условиям реализации основной профессиональной образовательной программы

Реализация основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» обеспечивается педагогическими работниками университета, а также лицами, привлекаемыми университетом к реализации основной профессиональной образовательной 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 основной профессиональной образовательной программы, и лиц, привлекаемых университетом к реализации основной профессиональной образовательной программы на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), ведут научную, учебно-методическую и (или) практическую работу, соответствующую профилю

Согласована на портале № 1529

преподаваемой дисциплины (модуля).

Не менее 3 процентов численности педагогических работников университета, участвующих в реализации основной профессиональной образовательной программы, и лиц, привлекаемых университетом к реализации основной профессиональной образовательной 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).

Не менее 50 процентов 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).

Доля педагогических работников ТУСУРа (исходя из количества замещаемых ставок, приведенного к целочисленным значениям) составляет не менее 55 процентов от общего количества лиц, привлекаемых к реализации программы бакалавриата. В реализации программы бакалавриата принимает участие минимум один педагогический работник, 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".

6.4. Требования к финансовым условиям реализации основной профессиональной образовательной программы

Финансовое обеспечение реализации основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» осуществляется в объеме не ниже значений базовых нормативов затрат на оказание государственных услуг по реализации образовательных программ высшего образования и значений корректирующих коэффициентов к базовым нормативам затрат, определяемых Минобрнауки России.

6.5. Требования к применяемым механизмам оценки качества образовательной деятельности и подготовки обучающихся по основной профессиональной образовательной программе

Качество образовательной деятельности и подготовки обучающихся по основной профессиональной образовательной программе по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» определяется в рамках системы внутренней оценки, а также системы внешней оценки, в которой университет принимает участие на добровольной основе.

В целях совершенствования основной профессиональной образовательной программы

Согласована на портале № 1529

университет при проведении регулярной внутренней оценки качества образовательной деятельности и подготовки обучающихся по основной профессиональной образовательной программе 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 основной профессиональной образовательной программе 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 основной профессиональной образовательной программе в рамках процедуры государственной аккредитации осуществляется с целью подтверждения соответствия образовательной деятельности по основной профессиональной образовательной программе требованиям ФГОС ВО.

Внешняя оценка качества образовательной деятельности и подготовки обучающихся по основной профессиональной образовательной программе может осуществляться 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.

6.6. Условия реализации основной профессиональной образовательной программы для инвалидов и лиц с ограниченными возможностями здоровья

При наличии в контингенте обучающихся по основной профессиональной образовательной программе по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Безопасность компьютерных систем» инвалидов и лиц с ограниченными возможностями здоровья по личному заявлению обучающихся основная профессиональная образовательная программа адаптируется с учетом особенностей их психофизического развития, индивидуальных возможностей и при необходимости обеспечивает коррекцию нарушений развития и социальную адаптацию указанных лиц.

Срок получения образования по адаптированной образовательной программе при обучении по индивидуальному учебному плану инвалидов и лиц с ОВЗ может быть увеличен по их заявлению не более чем на 1 год по сравнению со сроком получения образования, установленным во ФГОС ВО для соответствующей формы обучения.

Для инвалидов и лиц с ограниченными возможностями здоровья устанавливается особый порядок освоения дисциплин (модулей) по физической культуре и спорту с учетом состояния их здоровья.

Для лиц с ограниченными возможностями здоровья выбор мест прохождения практик учитывает состояние здоровья и требования по доступности.

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

Важным фактором социальной адаптации обучающихся с ограниченными возможностями

Согласована на портале № 1529

здоровья и инвалидов является индивидуальное сопровождение, которое имеет непрерывный и комплексный характер.

Сопровождение привязано к структуре образовательного процесса, определяется его целями, построением, содержанием и методами, имеет предупреждающий характер и особенно актуально, когда у обучающихся с ограниченными возможностями здоровья и обучающихся инвалидов возникают проблемы учебного адаптационного, коммуникативного характера, препятствующие своевременному формированию необходимых компетенций.

Сопровождение включает в себя:

– организационно-педагогическое сопровождение, которое направлено на контроль учебы обучающихся с ограниченными возможностями здоровья и инвалидов в соответствии с графиком учебного процесса в условиях инклюзивного обучения;

– психолого-педагогическое сопровождение, которое осуществляется для обучающихся с ограниченными возможностями здоровья и инвалидов, имеющих проблемы в обучении, общении и социальной адаптации, и направлено на изучение, развитие и коррекцию личности обучающегося и адекватность формирования компетенций;

– профилактически-оздоровительное сопровождение, которое предусматривает решение задач, направленных на повышение адаптационных возможностей обучающихся с ограниченными возможностями здоровья и инвалидов, гармонизацию их психического состояния, профилактику обострений основного заболевания, а также на нормализацию фонового состояния, что снижает риск обострения основного заболевания;

– социальное сопровождение, решающее широкий спектр задач социального характера, от которых зависит успешная учеба обучающихся с ограниченными возможностями здоровья и обучающихся инвалидов. Это содействие в решении бытовых проблем, транспортных вопросов, социальные выплаты, выделение материальной помощи, организация досуга, летнего отдыха, вовлечение их в студенческое самоуправление, организация волонтерского движения и др.

Согласована на портале № 1529

infotecs
Акционерное общество
«Информационные технологии
и коммуникационные системы»
(АО «ИнфоТеКС»)
Юридический адрес:
ул. Викторенко, д. 9, стр. 1, помещ. 47
вн.тер.г. муниципальный округ Хорошевский,
Москва, 125167
Почтовый адрес:
а/я №80, улица Отрадная, дом 2Б, стр. 1
Москва, 127273
Тел. (495)737-61-92, факс (495)737-72-78
e-mail: soft@infotecs.ru
http://www.infotecs.ru
ОГРН 1027739185066
ИНН/КПП 7710013769/771401001

– 8 СЕН 2026 № И-2026-0837/1

Ректору
ФГАОУ ВО «ТУСУР»
Рулевскому В.М.

пр. Ленина, 40, г. Томск, 634050
тел. (382 2) 510-530
факс (382 2) 513-262, 526-365
e-mail:office@tusur.ru
http://www.tusur.ru

002695

РЕЦЕНЗИЯ

на основную профессиональную образовательную программу высшего образования (ОПОП ВО)

по направлению подготовки **10.03.01 Информационная безопасность** направленности (профиля) бакалавриата **«Безопасность компьютерных систем»**, ФГОС ВО 3++, реализуемую в Томском государственном университете систем управления и радиоэлектроники (ТУСУР) на кафедре комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)

Основная профессиональная образовательная программа имеет типовую структуру, содержащую разделы с обязательными сведениями: общие положения с характеристиками основной образовательной программы, перечень квалификационных характеристик выпускника, включая область, объекты, виды и задачи профессиональной деятельности, анализ требований профессиональных стандартов, учебный план, рабочие программы дисциплин, программы практик, программу государственной итоговой аттестации. Также определены общесистемные требования, кадровые условия, материально-техническое обеспечение и финансовые условия реализации основной образовательной программы **10.03.01 Информационная безопасность** направленности (профиля) **«Безопасность компьютерных систем»**, ФГОС ВО 3++.

Цели ОПОП по направлению подготовки **10.03.01 Информационная безопасность** соответствуют запросам работодателей в области обеспечения информационной безопасности, целям и задачам обеспечения технологического лидерства, требованиям образовательного стандарта и миссии высшего учебного заведения. Программа реализована на уровне «ТОП ИТ "СТАРТ"» и ориентирована на подготовку конкурентоспособных специалистов, способных осуществлять полный цикл проектирования и эксплуатации защищённых информационных систем.

Перечень осваиваемых обучающимися компетенций учитывает все требования ФГОС ВО 3++ по направлению подготовки **10.03.01 Информационная безопасность,** утвержденному приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427, для профиля бакалавриата **«Безопасность компьютерных систем».**

Согласована на портале № 1529

Дисциплины учебного плана обеспечивают формирование у выпускников комплексных знаний и практических навыков в области защиты информации, в том числе в сфере безопасности компьютерных сетей и криптографических методов защиты данных. Рабочие программы дисциплин соответствуют типовой структуре и содержат все обязательные элементы: цели и задачи, требования к результатам освоения, объёмы и содержание по видам занятий, перечень формируемых компетенций, рейтинговую систему оценки успеваемости, учебно-методические материалы, сведения о программном и материально-техническом обеспечении, оценочные материалы и методические рекомендации.

АО «ИнфоТеКС», выступающее якорным индустриальным партнёром образовательной программы, является одним из ведущих отечественных разработчиков и производителей высокотехнологичных программных и программно-аппаратных средств защиты информации, включая средства криптографической защиты, продукты класса VPN и решения по защите объектов критической информационной инфраструктуры. В рамках многолетнего сотрудничества компания обеспечивает системное участие в реализации программы: ведёт профильные дисциплины, организует учебные практики и стажировки на реальных производственных задачах, а также предоставляет программно-аппаратные комплексы и учебные лицензии для работы с продуктами линейки ViPNet. С позиции АО «ИнфоТеКС», ОПОП в полной мере учитывает современные требования отрасли к подготовке специалистов в области сетевой безопасности и криптографической защиты информации: содержание профильных дисциплин охватывает принципы построения защищённых сетевых инфраструктур, применение отечественных криптографических алгоритмов и сертифицированных средств защиты информации, а также практику работы с реальными средствами обеспечения безопасности телекоммуникационных систем. Программа формирует у выпускников компетенции, востребованные при решении как актуальных задач защиты программных продуктов, так и перспективных задач по интеграции механизмов безопасности в современные архитектуры разработки и эксплуатации.

Реализуемая совместно с партнерами блочная структура образовательной программы является ядром профилирования и формирует доменные и опережающие компетенций будущего выпускника, что особенно актуально в связи экспоненциальным ростом уровня угроз информационной безопасности и выраженным дефицитом квалифицированных специалистов.

В рамках программы предусмотрены актуальные и прогрессивные образовательные форматы, позволяющие обеспечивать эффективный трансфер научного знания в прикладные перспективные решения.

Программой предусматривается создание совместно с индустриальными партнёрами открытых платформ, площадок и форматов на базе университета, направленных в том числе на раннюю интеграцию активных обучающихся в профессиональное сообщество.

Важным аспектом программы являются механизмы регулярной актуализации учебных материалов, формируемых на основе реальных производственных задач индустриальных партнёров, реализуемые на протяжении всего периода обучения.

Программа государственной итоговой аттестации по направлению подготовки **10.03.01 Информационная безопасность** позволяет полностью оценить уровень подготовки выпускника для выполнения профессиональных задач и позволяет установить соответствие итоговых полученных знаний, умений и навыков ФГОС ВО 3++.

Имеющееся в ВУЗе обеспечение соответствует всем требованиям ФГОС ВО 3++, образовательная структура ВУЗа позволяет обеспечить полноценную подготовку и развитие будущего выпускника.

Согласована на портале № 1529

Можно сделать заключение, что основная профессиональная образовательная программа **10.03.01 Информационная безопасность** полностью соответствует требованиям ФГОС ВО 3++ и ожиданиям отраслевого контура, может быть использована в рамках учебного процесса ТУСУРа на уровне «ТОП ИТ "СТАРТ"».

Рецензент:
Руководитель Центра научных исследований
и перспективных разработок, к.т.н. В.Л. Елисеев



Согласована на портале № 1529

АО "Аладдин Р.Д."
129226, Москва, ул. Докукина, д. 16, стр. 1
эт. 7, пом. 1, ком 22
Тел.: +7 (495) 223-00-01
Факс: +7 (495) 646-08-82
E-mail: aladdin@aladdin-rd.ru
Web: www.aladdin-rd.ru

РЕЦЕНЗИЯ

на основную профессиональную образовательную программу высшего образования (ОПОП ВО)

по направлению подготовки **10.03.01 Информационная безопасность** направленности (профиля) бакалавриата **«Безопасность компьютерных систем»**, ФГОС ВО 3++, реализуемую в Томском государственном университете систем управления и радиоэлектроники (ТУСУР) на кафедре комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)

Основная профессиональная образовательная программа имеет типовую структуру, содержащую разделы с обязательными сведениями: общие положения с характеристиками основной образовательной программы, перечень квалификационных характеристик выпускника, включая область, объекты, виды и задачи профессиональной деятельности, анализ требований профессиональных стандартов, учебный план, рабочие программы дисциплин, программы практик, программу государственной итоговой аттестации. Также определены общесистемные требования, кадровые условия, материально-техническое обеспечение и финансовые условия реализации основной образовательной программы **10.03.01 Информационная безопасность** направленности (профиля) **«Безопасность компьютерных систем»**, ФГОС ВО 3++.

Цели ОПОП по направлению подготовки **10.03.01 Информационная безопасность** соответствуют запросам работодателей в области обеспечения информационной безопасности, требованиям образовательного стандарта и миссии высшего учебного заведения. Программа соответствует уровню «ТОП ИТ "СТАРТ"» и направлена на подготовку специалистов, готовых к решению полного цикла задач в сфере защиты компьютерных систем и обеспечения безопасной разработки программного обеспечения.

Перечень осваиваемых обучающимися компетенций учитывает все требования ФГОС ВО 3++ по направлению подготовки **10.03.01 Информационная безопасность,** утверждённому приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427, для профиля бакалавриата **«Безопасность компьютерных систем»**.

Дисциплины учебного плана позволяют получить все необходимые навыки в области защиты компьютерных систем, в том числе в сфере управления доступом, механизмов аутентификации и авторизации пользователей и программных компонентов. Рабочие программы дисциплин соответствуют типовой структуре и содержат все обязательные элементы: цели и задачи, требования к результатам освоения дисциплин, объёмы и содержание по видам занятий, перечень формируемых компетенций, рейтинговую систему оценивания, учебно-методические материалы, сведения о программном и материально-техническом обеспечении, оценочные материалы и методические рекомендации. Практическая подготовка реализуется через систему сквозных промышленных кейсов на реальных

Согласована на портале № 1529

задачах индустриальных партнёров, что обеспечивает накопление выпускником подтверждённого портфеля практических результатов.

АО «Аладдин Р.Д.», принимающее участие в реализации образовательной программы в роли индустриального партнёра, является российским разработчиком средств строгой аутентификации, защищённого доступа и решений в области доверенного взаимодействия компонентов информационных систем. Компетенции компании в части средств строгой аутентификации, защищённого доступа к конечным точкам и обеспечения доверенного взаимодействия компонентов промышленной автоматизации обеспечивают расширение содержательного контура программы в направлениях, связанных с защитой критической информационной инфраструктуры и доверенными вычислениями. С позиции АО «Аладдин Р.Д.», ОПОП в полной мере отражает актуальные требования рынка к подготовке специалистов в области разграничения доступа и аутентификации: содержание профильных дисциплин охватывает современные модели и механизмы управления доступом, включая ролевые и мандатные модели, многофакторную и строгую аутентификацию, применение смарт-карт и аппаратных токенов, а также принципы построения систем защищённого удалённого доступа и реализации концепции нулевого доверия (Zero Trust). Участие компании в программе позволяет обогатить практическую составляющую подготовки актуальными сценариями применения сертифицированных отечественных средств защиты информации в корпоративных и промышленных инфраструктурах.

Программа государственной итоговой аттестации по направлению подготовки **10.03.01 Информационная безопасность** позволяет полностью оценить уровень подготовки выпускника для выполнения профессиональных задач и позволяет установить соответствие итоговых полученных знаний, умений и навыков ФГОС ВО 3++.

Имеющееся в ВУЗе обеспечение соответствует всем требованиям ФГОС ВО 3++, образовательная структура ВУЗа позволяет обеспечить полноценную подготовку и развитие будущего выпускника.

Можно сделать заключение, что основная профессиональная образовательная программа **10.03.01 Информационная безопасность** полностью соответствует требованиям ФГОС ВО 3++ и может быть использована в рамках учебного процесса ТУСУРа.

Рецензент:
Первый заместитель
генерального директора АО «Аладдин Р.Д.» _____ О.А. Панарин

09.09.2026 г.

Согласована на портале № 1529

Лист согласования
основной профессиональной образовательной программы высшего образования
- программы бакалавриата по направлению подготовки
10.03.01 Информационная безопасность
направленности (профилю)
«Безопасность компьютерных систем»

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол от 10.07.2026 № 12

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Руководитель образовательной программы, доцент каф. КИБЭВС, кандидат технических наук, доцент	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Заведующий каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Декан ФБ	Е.М. Давыдова	Согласовано, d4acdfdc-18d3-41a1-ac4e-4a426c6b834a
Представители работодателей:		
ООО "Юзергейт", ведущий инженер-разработчик	А.И. Гуляев	Согласовано, 3b8c1617-2959-db02-a552-a3d72681fe71
АО "Аладдин Р.Д.", директор по инновационным проектам, кандидат технических наук	О.Н. Дьяков	Согласовано, 96f63e71-9a86-4d1f-65ad-3f3b4f1f723c
АО "Инфотекс", руководитель центра научных исследований и перспективных разработок, кандидат технических наук	В.Л. Елисеев	Согласовано, 7cf6fef4-6bb1-49b1-3239-77f2436b7de3
РАЗРАБОТАНО:		
Доцент каф. КИБЭВС, кандидат технических наук	А.Ю. Якимук	Разработано, 4ffdf265-fb78-4863-b293-f03438cb07cc

Согласована на портале № 1529

Должность	Инициалы, фамилия	Подпись
Доцент каф. КИБЭВС, кандидат технических наук, доцент	А.А. Конев	Разработано, 81687a04-85ce-4835-9e1e-9934a6085fdd

Согласована на портале № 1529