МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный геологоразведочный университет имени Серго Орджоникидзе»

(МГРИ)

СОГЛАСОВАНО
Проректор по образовательной деятельности
_____ Л.В. Куклина
«27» марта 2025 г.

УТВЕРЖДЕНО
Ученым советом университета
Протокол № 7 от «27» марта 2025 г.
Председатель Ученого совета
_____ Ю.П. Панов

ОСНОВНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ – ПРОГРАММА СПЕЦИАЛИТЕТА

Специальность: 10.05.03 Информационная безопасность автоматизированных систем
Квалификация: Специалист по защите информации
Специализация: Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)
Типы задач профессиональной деятельности: научно-исследовательский, проектный, контрольно-аналитический, организационно-управленческий, эксплуатационный
Сроки получения образования по программе специалитета:
очная форма обучения – 5 лет 6 месяцев
Форма обучения: очная

Москва 2025

СОДЕРЖАНИЕ:

4.	**ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**
4.1.	Компетенции выпускника, формируемые в результате освоения ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)
4.2.	Матрица соответствия планируемых программных результатов обучения по ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)
5.	**ОБЪЁМ И СТРУКТУРА ОПОП ВО по специальности** 10.05.03 Информационная безопасность автоматизированных систем **специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**
6.	**ПОРЯДОК ОРГАНИЗАЦИИ ПРАКТИЧЕСКОЙ ПОДГОТОВКИ ОБУЧАЮЩИХСЯ, осваивающих ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**
7.	**ТРЕБОВАНИЯ И ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**
7.1.	Общесистемные требования к реализации ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**

7.2.	Требования к материально-техническому и учебно-методическому обеспечению ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**
7.3.	Требования к кадровым условиям реализации ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**
7.4.	Требования к финансовым условиям реализации ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**
8.	**ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ для лиц с ограниченными возможностями здоровья при освоении ими ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**
9.	**ХАРАКТЕРИСТИКА ВОСПИТАТЕЛЬНОЙ СРЕДЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ**
10.	**ОЦЕНКА КАЧЕСТВА ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ И ПОДГОТОВКИ ОБУЧАЮЩИХСЯ по ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**
11.	**РЕГЛАМЕНТ ПО ОРГАНИЗАЦИИ ПЕРИОДИЧЕСКОГО ОБНОВЛЕНИЯ ОПОП ВО по специальности 00.00.00 Наименование специализация - Наименование в целом, а также составляющих ее компонентов**

12.	**ПРИЛОЖЕНИЯ, определяющие содержание ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**
12.1.	*Приложение 1. Структурная матрица формирования компетенций в соответствии с ФГОС ВО по ОПОП ВО по специальности* **10.05.03 Информационная безопасность автоматизированных систем специализация** *(специализация* **- Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**
12.2.	*Приложение 2. Компетентностно-ориентированный учебный план для обучающихся очной формы обучения*
12.3	*Приложение 3. Календарный учебный график для обучающихся очной формы обучения*
12.4.	*Приложение 4. Программа государственной итоговой аттестации (ГИА), включающая форму аттестации*
12.5.	*Приложение 5. Рабочие программы дисциплин (модулей), включающие фонды оценочных средств*
12.6.	*Приложение 6. Программы практик, включающие фонды оценочных средств*
12.7.	*Приложение 7. Программа научно-исследовательской работы, включающая фонды оценочных средств*
12.8	*Приложение 8. Рабочая программа воспитания*
12.9.	*Приложение 9. Календарный план воспитательной работы для обучающихся очной формы обучения*
12.10.	*Приложение 10. Методические рекомендации по выполнению выпускной квалификационной работы*
12.11.	*Приложение 11. Методические указания по освоению дисциплин*

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ:

ФГОС ВО - Федеральный государственный образовательный стандарт высшего образования;

ПС - профессиональный стандарт;

ОПОП ВО - основная профессиональная образовательная программа высшего образования - программа специалитета;

УК - универсальная компетенция;

ОПК - общепрофессиональная компетенция;

ПК - профессиональная компетенция;

ОТФ - обобщенная трудовая функция;

ТФ - трудовая функция;

ТД - трудовое действие;

НУ- необходимое умение;

НЗ - необходимое знание;

УП - учебный план;

ИУП- индивидуальный учебный план;

РПД - рабочая программа дисциплины;

ВКР - выпускная квалификационная работа;

ГИА - государственная итоговая аттестация;

з.е. - зачетные единицы трудоемкости;

ОВЗ - ограниченные возможности здоровья;

ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) представляет собой комплекс 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.

Обучение по программе специалитета в образовательной организации может осуществляться в **очной форме.*

Срок получения образования по программе специалитета (вне зависимости от применяемых образовательных технологий):

в очной форме обучения**, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет **5,5 лет.

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

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение основной профессиональной образовательной программы высшего образования - программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем

(*далее - ОПОП ВО по специальности* **10.05.03 Информационная безопасность автоматизированных систем**)

(специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности))

Основная профессиональная образовательная программа высшего образования - программа специалитета по специальности **10.05.03 Информационная безопасность автоматизированных систем**.

Специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности).

Квалификация, присваиваемая выпускникам – **специалист по защите информации**.

Назначение ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; формы обучения: очная) отражено в комплексе основных характеристик образования (объем, содержание, планируемые результаты) и организационно-педагогических условий, который представлен в виде учебного плана, календарного учебного графика рабочих программ дисциплин (модулей), программы государственной итоговой аттестации, иных компонентов, оценочных и методических материалов, а также в виде рабочей программы воспитания, календарного плана воспитательной работы, форм аттестации, разработанным и утвержденным Федеральным государственным бюджетным образовательным учреждением высшего образования «Российский государственный геологоразведочный университет имени Серго Орджоникидзе (*далее - МГРИ, образовательная организация*) по специальности **10.05.03 Информационная безопасность автоматизированных систем** на основе федерального государственного образовательного стандарта высшего образования - специалитет по специальности **10.05.03 Информационная безопасность автоматизированных систем**, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1457 (зарегистрирован Министерством юстиции Российской Федерации 17 февраля

2021 г., регистрационный № 62532), с учетом требований профессиональных стандартов - подготовка выпускника, который способен, опираясь на полученные углубленные знания, умения и сформированные компетенции, самостоятельно решать на современном уровне задачи в области профессиональной деятельности с учетом потребностей российского рынка труда.

ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) регламентирует цели, ожидаемые результаты, содержание, условия и технологии реализации образовательного процесса, оценку качества подготовки выпускника по данному направлению подготовки и включает в себя выше перечисленные обязательные компоненты, обеспечивающие качество подготовки обучающихся-выпускников и их конкурентоспособность, а также применяемые в МГРИ образовательные технологии.

При реализации ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) образовательная организация вправе применять электронное обучение и дистанционные образовательные технологии. Образовательная деятельность по ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности); форма обучения: очная) осуществляется на государственном языке (русском языке) Российской Федерации.

Наиболее целесообразно использование выпускников, освоивших ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем (**специализация **- Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности); формы обучения: очная**) на предприятиях минерально-сырьевого комплекса, деятельность которых связана с горнодобывающей промышленностью и геологоразведкой.

Социальная значимость ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем (**специализация **- Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) состоит в развитии инновационного человеческого капитала на основе тесной интеграции образовательного, научного, воспитательного и профориентационного процессов во благо граждан и общества и для процветания Российской Федерации.

1.2. Нормативные документы для разработки ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)

Нормативной базой для разработки основной профессиональной образовательной программы по специальности **10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности);** форма обучения: очная) являются:

- Указ Президента Российской Федерации от 28.02.2024 № 145 «О Стратегии научно-технологического развития Российской Федерации»;
- Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») с изменениями и дополнениями от 15.02.2024;
- Указ Президента Российской Федерации от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»;
- Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 28.12.2024) «Об образовании в Российской Федерации»;
- Федеральный закон от 31.07.2020 № 304-ФЗ «О внесении изменений в Федеральный закон об образовании в Российской Федерации по вопросам воспитания обучающихся»;
- Федеральный закон от 27.07.2006 № 149-ФЗ (*ред. от 23.11.2024*) «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ (*ред. от 08.08.2024*) «О персональных данных»;
- Постановление Правительства Российской Федерации от 16.11.2020 № 1836 «О государственной информационной системе "Современная цифровая образовательная среда"» (вместе с «Положением о государственной информационной системе "Современная цифровая образовательная среда»);

- Постановление Правительства Российской Федерации от 20.10.2021 № 1802 «Об утверждении правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации, а также о признании утратившими силу некоторых актов и отдельных положений некоторых актов правительства Российской Федерации»;

- Приказ Федеральной службы по надзору в сфере образования и науки от 04.08.2023 № 1493 «Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления информации»;

- Приказ Минобрнауки РФ от 26.11.2020 № 1457 «Об утверждении федерального государственного образовательного стандарта высшего образования - специалитет по специальности **10.05.03 Информационная безопасность автоматизированных систем** (зарегистрирован Минюстом России 17.02.2021 № 62532), (*далее - ФГОС ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем)***;

- Приказ Минобрнауки России от 12.09.2013 № 1061 «Об утверждении перечней специальностей и направлений подготовки высшего образования» (в редакции от 13.12.2021);

- Приказ Минобрнауки России от 06.04.2021 № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры» (зарегистрирован Минюстом России 13.08.2021 № 64644);

- Приказ Минобрнауки России № 885, Минпросвещения России № 390 от 05.08.2020 (*ред. от 18.11.2020*) «О практической подготовке обучающихся» (вместе с «Положением о практической подготовке обучающихся») (зарегистрирован Минюстом России 11.09.2020 № 59778);

- Приказ Минобрнауки России от 29.06.2015 № 636 (*ред. от 27.03.2020*) «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры» (зарегистрирован Минюстом России 22.07.2015 № 38132);

- Приказ Минобрнауки России от 09.11.2015 № 1309 (*ред. от 18.08.2016*) «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи» (зарегистрирован Минюстом России 08.12.2015 № 40000);

- Приказ Минобрнауки России от 08.02.2021 № 84 «О внесении изменений в федеральные государственные образовательные стандарты высшего образования – специалитет по специальностям» (зарегистрирован Минюстом России 12.03.2021 № 62736);

- Приказ Минобрнауки России от 19.07.2022 № 662 «О внесении изменений в федеральные государственные образовательные стандарты высшего образования» (зарегистрирован Минюстом России 07.10.2022 № 70414);

- Приказ Минобрнауки России от 27.02.2023 № 208 «О внесении изменений в федеральные государственные образовательные стандарты высшего образования» (зарегистрирован Минюстом России 31.03.2023 № 72833);

- Письмо Министерства науки и высшего образования от 21.04.2023 № МН-11/1516-ПК;

- Письмо Министерства науки и высшего образования от 14.06.2023 № МН-5/179660;

- Письмо Министерства науки и высшего образования от 14.06.2023 № МН-11/418-ОП;

- Устав ФГБОУ ВО «Российский государственный геологоразведочный университет имени Серго Орджоникидзе»;

- Иные локальные нормативные акты ФГБОУ ВО «Российский государственный геологоразведочный университет имени Серго Орджоникидзе».

Основная профессиональная образовательная программа высшего образования - программа специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная, разработана также с учётом рабочей программы воспитания обучающихся, календарного плана воспитательной работы на 2025/2026 учебный год.

Практическая подготовка обучающихся организована образовательной организацией при реализации учебных дисциплин, практик (контактная работа педагогического работника с обучающимся), иных компонентов основной профессиональной образовательной программы высшего образования - программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная), в условиях выполнения

обучающимися определённых видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие соответствующих практических навыков и компетенций.

2. ХАРАКТЕРИСТИКА ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)

2.1. Общая характеристика ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности))

Миссия ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная):

- формирование высококвалифицированного и конкурентоспособного компетентного выпускника, востребованного на рынке труда, владеющего знаниями в сфере обеспечения безопасности информации в автоматизированных системах, способного решать задачи профессиональной деятельности;
- развитие у обучающегося качеств, направленных в том числе на освоение сквозных цифровых технологий в профессиональной деятельности выпускника;
- обеспечение расширенного воспроизводства интеллектуальных ресурсов для минерально-сырьевого комплекса, как важнейшего фактора устойчивого развития Российской Федерации, и удовлетворение народного хозяйства страны в высококвалифицированных кадрах в области информационной безопасности.

Для выполнения **миссии** необходимо реализовать следующие основные **цели**:

Образовательная цель - подготовка квалифицированных специалистов, обладающих профессиональными навыками, позволяющим выпускнику

успешно работать в избранной сфере деятельности, на основе достижений теории и практики, с использованием в профессиональной деятельности информационно-коммуникационных технологий; обладать универсальными (УК), общепрофессиональными (ОПК) и профессиональными (ПК) компетенциями (*профессиональные компетенции определены образовательной организацией самостоятельно на основе обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники, с учетом мнения экспертов из числа представителей заинтересованных организаций и иных источников),* способствующими его социальной мобильности и конкурентоспособности на рынке труда с учётом специфики региона.

Воспитательная цель - развитие у обучающегося личностных качеств, а также реализация компетентностного подхода, индивидуальная работа с каждым обучающимся, формирование у него универсальных компетенций (УК), общепрофессиональных компетенций (ОПК), а также профессиональных компетенций (ПК) (*профессиональные компетенции определены образовательной организацией самостоятельно на основе обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники, с учетом мнения экспертов из числа представителей заинтересованных организаций и иных источников),* направленных на формирование у обучающегося сознательного отношения к получению профессиональных знаний и навыков, потребности и умения учиться и трудиться; использование воспитательного потенциала учебных предметов для расширения культурного кругозора обучающихся, их творческой и социальной активности; подготовка конкурентоспособных кадров, обладающих высоким уровнем социально-личностных и профессиональных компетенций.

Развивающая цель - способствовать формированию личности достойного гражданина, развитию интеллектуальной сферы, раскрытию разносторонних творческих возможностей обучаемого, формированию системы ценностей, потребностей, стремлений в построении успешной карьеры.

В области **профессиональной подготовки** специалистов **решаются следующие задачи:**

- формирование личности, способной на основе полученных знаний, умений, владений в области информационной безопасности, а также на основе сформированных в процессе освоения ОПОП ВО универсальных (УК), общепрофессиональных (ОПК), профессиональных компетенций (ПК)

(*профессиональные компетенции определены образовательной организацией самостоятельно на основе обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники, с учетом мнения экспертов из числа представителей заинтересованных организаций и иных источников),* способствовать повышению качества и эффективности работ по защите информации.

- освоение новейших подходов и методик по защите информации и принятии компетентных проектных и управленческих решений;

- развитие у обучающихся способностей и профессиональных навыков в области организационно-управленческой деятельности по следующим направлениям: связь, информационные и коммуникационные технологии в сфере обеспечения безопасности информации в автоматизированных системах;

- развитие высокой компетентности, в том числе в цифровой среде, инициативности и умения творчески подходить к делу при решении задач, стоящих перед экономикой страны, в том числе цифровой;

- подготовка выпускника, обладающего глубокой фундаментальной теоретической и практической подготовкой в области информационной безопасности.

Срок получения образования по ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) (вне зависимости от применяемых образовательных технологий):

в очной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет **5,5 лет**;

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

Объем ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) составляет 330 зачетных единиц (*далее - з.е.*) вне зависимости от формы обучения, применяемых образовательных технологий, реализации ОПОП ВО по специальности 10.05.03 Информационная безопасность

автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) с использованием сетевой формы, реализации ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) по индивидуальному учебному плану.

Объем ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная), реализуемый за один учебный год, составляет не более 70 з.е. вне зависимости от формы обучения, применяемых образовательных технологий, реализации ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), формы обучения: очная) с использованием сетевой формы, реализации ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), формы обучения: очная) по индивидуальному учебному плану (за исключением ускоренного обучения), а при ускоренном обучении - не более 80 з.е.

Образовательная деятельность по ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) осуществляется на государственном языке Российской Федерации.

2.2. Требования к уровню подготовки абитуриента, необходимому для освоения ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем

(специализация – Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности))

К освоению ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация – **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) допускаются лица, имеющие образование соответствующего уровня, подтвержденное при поступлении на обучение по программе специалитета - документом о среднем общем образовании или документом о среднем профессиональном образовании и о квалификации, или документом о высшем образовании и о квалификации.

При приеме абитуриентов на обучение по ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) образовательная организация руководствуется Порядком приема в МГРИ, разработанным и утвержденным в соответствии с требованиями Приказа Минобрнауки России от 27.11.2024 № 821 «Об утверждении Порядка приема на обучение по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры» (зарегистрирован Минюстом России 29.11.2024 № 80379).

3. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКА

При разработке ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем, форма обучения: очная образовательной организацией установлена специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**, которая конкретизирует содержание программы специалитета в рамках направления подготовки путем ориентации ее на:

- области профессиональной деятельности и сферы профессиональной деятельности выпускников;
- типы задач профессиональной деятельности выпускников;
- объекты профессиональной деятельности выпускников.

3.1. Области и сферы профессиональной деятельности выпускника

Области профессиональной деятельности и сферы профессиональной деятельности в которых выпускники, освоившие ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем

(специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная), могут осуществлять профессиональную деятельность:

01 Образование и наука (в сфере научных исследований); 06 Связь, информационные и коммуникационные технологии (в сфере обеспечения безопасности информации в автоматизированных системах); 12 Обеспечение безопасности (в сфере обеспечения безопасности информации в автоматизированных системах, обладающих информационно-технологическими ресурсами, подлежащими защите); сфера обороны и безопасности; сфера правоохранительной деятельности.

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

3.2. Объекты профессиональной деятельности выпускника

Объектами профессиональной деятельности выпускников, освоивших программу специалитета 10.05.03 Информационная безопасность автоматизированных систем (специализация – Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)) являются:

- объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;
- угрозы безопасности информации, обрабатываемой объектами критической информационной инфраструктуры;
- меры и средства, используемые для обеспечения безопасности значимых объектов критической информационной инфраструктуры;
- система нормативных правовых актов, методических документов и национальных стандартов в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;
- субъекты критической информационной инфраструктуры Российской Федерации, функционирующие в области горнодобывающей промышленности (в части руд и камней);
- государственные и частные организации, занимающиеся процессами поиска, разведки, оценки, добычи, обогащения, логистики, поставки, рекультивации твердых и стратегических видов полезных ископаемых; строительства (сооружения) рудников и горно-обогатительных комбинатов (фабрик);

- государственные и частные организации, занимающиеся процессами разведки, добычи углеводородов; строительства, восстановления и реконструкции скважин на суше и море;
- иностранные горнодобывающие и геологоразведочные компании;
- научно-исследовательские и проектные организации и учреждения;
- другие объекты смежных видов профессиональной деятельности.

3.3. Типы задач профессиональной деятельности выпускника

В рамках освоения ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) выпускники готовятся к решению задач профессиональной деятельности **следующих типов**: научно-исследовательский; проектный; контрольно-аналитический; организационно-управленческий; эксплуатационный, исходя из потребностей рынка труда и цифровой экономики, научно-исследовательских и материально-технических ресурсов организации.

Программа специалитета формируется организацией в зависимости от типов задач учебной деятельности и требований к результатам освоения ОПОП ВО по направлению подготовки, ориентированной на научно-исследовательский, проектный, контрольно-аналитический, организационно-управленческий, эксплуатационный типы задач профессиональной деятельности как основные.

3.4. Задачи профессиональной деятельности

Выпускник должен быть подготовлен к решению профессиональных задач в соответствии со специализацией ОПОП ВО 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) и типами задач его будущей профессиональной деятельности.

Задачи профессиональной деятельности выпускника сформулированы на основе:

- ФГОС ВО – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Минобрнауки РФ от 26.11.2020 № 1457 (зарегистрирован Минюстом России 17.02.2021, регистрационный № 62532);

- обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники, с учетом мнения экспертов из числа представителей заинтересованных организаций и иных источников и дополнены с учётом традиций образовательной организации и потребностей заинтересованных работодателей, а именно:

в области научно-исследовательской деятельности:

- планирование и разработка мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

в области проектной деятельности:

- реализация мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

в области контрольно-аналитической деятельности:

- осуществление мер по контролю состояния безопасности значимых объектов критической информационной инфраструктуры;

в области организационно-управленческий деятельности:

- организация мероприятий по контролю состояния безопасности значимых объектов критической информационной инфраструктуры;

в области эксплуатационной деятельности:

- обеспечение функционирования систем безопасности значимых объектов критической информационной инфраструктуры;

3.5. Обобщённые трудовые функции выпускника

В соответствии с квалификационными требованиями, мнением экспертов из числа работодателей, анализа рынка труда, отечественного и зарубежного опыта, - выпускник должен овладеть следующими трудовыми функциями (Таблица № 1):

Таблица № 1

Обобщённые трудовые функции (код и наименование)	**Трудовые функции (код и наименование)**
Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	1 - Администрирование систем защиты информации автоматизированных систем; 2 - Управление защитой информации в автоматизированных системах; 3 - Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций; 4 - Мониторинг защищенности информации в автоматизированных системах; 5 - Аудит защищенности информации в автоматизированных системах; 6 - Разработка организационно- распорядительных документов по защите информации в автоматизированных системах;

	7 - Внедрение организационных мер по защите информации в автоматизированных системах;
Разработка систем защиты информации автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости	8 - Разработка проектных решений по защите информации в автоматизированных системах
Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости	9 - Моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности))

4.1 Компетенции выпускника, формируемые в результате освоения ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем

(специализация – **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**)

В результате освоения ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) у обучающегося формируются универсальные (УК), общепрофессиональные (ОПК), профессиональные (ПК) (*профессиональные компетенции определены образовательной организацией самостоятельно на основе обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники, с учетом мнения экспертов из числа представителей заинтересованных организаций и иных источников)* компетенции.

ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) устанавливает следующие **универсальные компетенции (УК)**:

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;

УК-2. Способен управлять проектом на всех этапах его жизненного цикла;

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели;

УК-4. Способен применять современные коммуникативные технологи, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия;

УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия;

УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни;

УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности;

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-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;

УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности.

ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) устанавливает следующие устанавливает следующие **общепрофессиональные компетенции (ОПК)**:

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-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;

ОПК-3. Способен использовать математические методы, необходимые для решения задач профессиональной деятельности;

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности;

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-7. Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;

ОПК-8. Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах;

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;

ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем;

ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;

ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;

ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико- экономического обоснования проектных решений;

ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;

ОПК-16. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма;

ОПК-11.1. Способен планировать и разрабатывать меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

ОПК-11.2. Способен обеспечивать функционирование систем безопасности значимых объектов критической информационной инфраструктуры;

ОПК-11.3. Способен организовывать и осуществлять меры по контролю состояния безопасности значимых объектов критической информационной инфраструктуры;

Профессиональные компетенции (ПК) (*профессиональные компетенции определены образовательной организацией самостоятельно на основе обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники, с учетом мнения экспертов из числа представителей заинтересованных организаций и иных источников)*.

Научно-исследовательский тип задач профессиональной деятельности:

ПК-1. Способен моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации;

Проектный тип задач профессиональной деятельности:

ПК-2. Способен разрабатывать проектные решения по защите информации в автоматизированных системах;

Контрольно-аналитический тип задач профессиональной деятельности:

ПК-3. Способен выполнять работы по мониторингу и аудиту защищенности информации в автоматизированных системах;

Организационно-управленческий тип задач профессиональной деятельности:

ПК-4. Способен разрабатывать организационно-распорядительные документы и внедрять организационные меры по защите информации в автоматизированных системах;

Эксплуатационный тип задач профессиональной деятельности:

ПК-5. Способен выполнять работы по администрированию систем защиты информации автоматизированных систем и обеспечивать их работоспособность при возникновении нештатных ситуаций;

ПК-6. Способен обнаруживать, идентифицировать и устранять инциденты, возникшие в процессе эксплуатации автоматизированных систем;

Совокупность компетенций, установленных ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) обеспечивает выпускнику способность осуществлять профессиональную деятельность в областях профессиональной деятельности и сферах профессиональной деятельности выпускников и решать задачи научно-исследовательского, проектного, контрольно-аналитического, организационно-управленческого, эксплуатационного типов профессиональной деятельности.

4.2. Матрица соответствия планируемых программных результатов обучения по ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности))

Образовательная организация самостоятельно установила в ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) индикаторы достижения компетенций.

Образовательная организация самостоятельно спланировала результаты обучения по дисциплинам (модулям) и практикам, которые соотнесены с установленными в ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная) индикаторами достижения компетенций.

Совокупность запланированных результатов обучения по дисциплинам (модулям) и практикам обеспечивает формирование у выпускника всех компетенций, установленных ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности), форма обучения: очная).

Таблица № 2

Компетенции		
универсальные компетенции (УК)		
Наименова-ние категории (группы) универсаль-ных компетенций	**код и наименование универсальной компетенции**	**код и наименование индикатора достижения универсальной компетенции**
Системное и критическое мышление	**УК-1.** Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	УК-1.1. ***Знать:*** структуру задач, выделяя ее базовые составляющие, осуществляет декомпозицию задачи;
		УК-1.2. ***Знать:*** основы поиска и анализа информации
		УК-1.2. ***Знать:*** основы системного подхода к решению задач профессиональной деятельности; взаимосвязь факторов, определяющих решение задач
		УК-1.4. ***Уметь:*** проводить поиск информации, необходимой для решения профессиональных задач. выявлять структуру задач, выделяя ее ключевые составляющие;
		УК-1.5. ***Уметь:*** Определять достоверность и надежность источников информации
		УК-1.6. ***Уметь:*** проводить анализ информации в соответствии с поставленными профессиональными задачами; определять возможные варианты решения задачи, оценивая их достоинства и недостатки; классифицировать факты, интерпретации, оценки в открытых и специализированных источниках информации;
		УК-1.7. ***Владеть:*** навыками аргументации на основе анализа информации при

		обсуждении подходов к решению профессиональных задач; навыками определения и оценки последствий возможных решений задачи;
		УК-1.8. ***Владеть:*** навыками диагностики поиска и критического анализа и синтеза информации, применяя системный подход для решения поставленных задач
		УК-1.9. ***Владеть:*** навыками определения и оценки последствий возможных решений задачи; навыками декомпозиции задачи; навыками разработки плана действий по решению поставленных задач;
Разработка и реализация проектов	**УК-2.** Способен управлять проектом на всех этапах его жизненного цикла.	УК-2.1. ***Знать:*** основы проектной деятельности; правила публичного представления результатов проектов; основные правовые нормы при проектировании и реализации проектов
		УК-2.2. ***Знать:*** Основы планирования и проектирования работ
		УК-2.3. ***Знать:*** Специфику проектной деятельности в профессиональной сфере; Ограничения и нормы, предусмотренные законодательством в профессиональной области, которые необходимо учитывать при проектировании и реализации проектов; Основы планирования и проектирования работ
		УК-2.4. ***Уметь:***

		проектировать решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений; определять в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение;
		УК-2.5. ***Уметь:*** Решать конкретные задач проекта заявленного качества и за установленное время;
		УК-2.6. ***Уметь:*** Публично представлять результаты решения конкретной задачи проекта
		УК-2.7. ***Владеть:*** навыками проектирования решений конкретной задачи проекта с учетом оптимальных способов ее решения на основе действующих правовых норм и имеющихся ресурсов и ограничений;
		УК-2.8. ***Владеть:*** методами реализации задач в зоне своей ответственности с учётом имеющихся ресурсов и ограничений, действующих правовых норм, при необходимости корректируя способы решения задач
		УК-2.9. ***Владеть:*** навыками публичного представления результатов решения конкретной задачи проекта и проекта в целом; навыками оформления результатов выполнения проекта

Командная работа и лидерство	**УК-3.** Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.	УК-3.1. ***Знать:*** основы стратегии сотрудничества для достижения поставленной цели,
		УК-3.2. ***Знать:*** особенности поведения выделенных групп людей, с которыми работает /взаимодействует, учитывает их в своей деятельности;
		УК-3.3. ***Знать:*** типологию и факторы формирования команд, способы социального взаимодействия
		УК-3.4. ***Уметь:*** эффективно взаимодействовать с другими членами команды, в т.ч. участвовать в обмене информацией, знаниями и опытом;
		УК-3.5. ***Уметь:*** планировать последовательность шагов и распределять работу в команде для достижения заданного результата; проводить дифференциацию задач и соответствующих исполнителей, опираясь на их особенности
		УК-3.6. ***Уметь:*** представлять публично результаты работы команды;
		УК-3.7. ***Владеть:*** навыками организационной работы для выполнения поставленных задач в научной и общественной деятельности
		УК-3.8. ***Владеть:*** методами планирования командной работы, навыками дифференциации задач и исполнителей в научной и общественной деятельности,
		УК-3.9. ***Владеть:*** способами оценивания результатов совместной работы,

		навыками составления отчетов о проделанной работе
Коммуникация	**УК-4.** Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия.	УК-4.1. ***Знать:*** стили делового общения на государственном (русском) и иностранном языках, вербальные и невербальные средства взаимодействия с партнерами; основы поиска необходимой информации с использованием информационно-коммуникационных технологий; основы перевода профессиональных текстов с иностранного (-ых) на государственный язык и обратно; основные коммуникативные технологии, применяемые для решения профессиональных задач, правила коммуникации в академических и профессиональных сообществах;
		УК-4.2. ***Знать:*** специальные коммуникативные технологии, применяемые для решения профессиональных задач, особенности коммуникации в профессиональных сообществах;
		УК-4.3. ***Знать:*** особенности технического перевода профессиональных текстов с иностранного (-ых) на государственный язык и обратно.
		УК-4.4. ***Уметь:*** ориентироваться при выборе приемлемых стилей делового общения в академическом и профессиональном сообществах; проводить поиск необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (-ых) языках;

		УК-4.5. ***Уметь:*** использовать стилистику делового общения в академическом и профессиональном сообществах; вести деловую переписку, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках;
		УК-4.6. ***Уметь:*** осуществлять перевод профессиональных и научных текстов с иностранного (-ых) на государственный язык и обратно
		УК-4.7. ***Владеть:*** навыками делового общения в профессиональной среде; навыками поиска необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (-ых) языках;
		УК-4.8. ***Владеть:*** Различными стилями делового общения и коммуникации в зависимости от специфики профессиональной и/или академической среды;
		УК-4.9. ***Владеть:*** навыками перевода профессиональных и научных текстов с иностранного (-ых) на государственный язык и обратно, навыками представления результатов профессиональной деятельности на различных публичных мероприятиях, включая международные, выбирая наиболее подходящий формат
Межкультурное взаимодействие	**УК-5.** Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия.	УК-5.1 ***Знать:*** этапы исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных

		традиций мира (в зависимости от среды и задач образования), включая религию, философские и этические учения;
		УК-5.2. ***Знать:*** историческое наследие и социокультурные традиции различных социальных групп; этапы исторического развития мировой цивилизации, включая основные события, основных исторических деятелей
		УК-5.3. ***Знать:*** мировые религии, философские и этические учения;
		УК-5.4. ***Уметь:*** находить и использовать необходимую для саморазвития и взаимодействия с другими информацию о культурных особенностях и традициях различных социальных групп
		УК-5.5. ***Уметь:*** недискриминационно и конструктивно взаимодействовать с людьми с учетом их социокультурных особенностей в целях успешного выполнения профессиональных задач и усиления социальной интеграции
		УК-5.6. ***Уметь:*** использовать знания исторических, этических и философских фактов для решения проблем мировоззренческого, нравственного и личностного характера, преодоления разногласий и конфликтов в межкультурной коммуникации
		УК-5.7. ***Владеть:*** недискриминационными и конструктивными способами взаимодействия с людьми с учетом их социокультурных особенностей
		УК-5.8. ***Владеть:*** недискриминационными и конструктивными способами взаимодействия с людьми с учетом

		их социокультурных особенностей в целях успешного выполнения профессиональных задач и усиления социальной интеграции
		УК-5.9. ***Владеть:*** Навыками взаимодействия с людьми с учетом их социокультурных особенностей в целях успешного выполнения профессиональных задач и усиления социальной интеграции
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	**УК-6.** Способен определять и реализовывать приоритеты собственной деятельности и способы её совершенствования на основе самооценки и образования в течение всей жизни.	УК-6.1. ***Знать:*** Условия и ограничения успешного выполнения порученной работы на основе собственных личностных, ситуативных, профессиональных качеств и возможности их совершенствования
		УК-6.2. ***Знать:*** Основы эффективного использования времени и других ресурсов при решении поставленных задач, а также относительно полученного результата;
		УК-6.3. ***Знать:*** инструменты и методы управления временем при выполнении конкретных задач, выстраивания траектории собственного профессионального роста
		УК-6.4. ***Уметь:*** Применять знания о своих ресурсах и их пределах (личностных, ситуативных, временных и т.д.), для успешного выполнения порученной работы;
		УК-6.5. ***Уметь:*** Определять приоритеты собственной деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда;
		УК-6.6.

		Уметь: Проводить оценку современных требований рынка труда для выстраивания траектории собственного профессионального развития
		УК-6.7. ***Владеть:*** информацией о потребностях рынка труда в образовательных услугах для выстраивания траектории собственного профессионального развития
		УК-6.8. ***Владеть:*** навыками реализации намеченных целей деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда
		УК-6.9. ***Владеть:*** Способами оценки эффективности использования времени и других ресурсов при решении поставленных задач, а также относительно полученного результата
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	**УК-7.** Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1 ***Знать:*** нормы здорового образа жизни; здоровьесберегающие технологии
		УК-7.2. ***Знать***: основы физической культуры; здоровьесберегающие технологии и возможности их применения с учетом внутренних и внешних условий реализации конкретной профессиональной деятельности
		УК-7.3. ***Знать***: организационную структуру физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки
		УК-7.4 ***Уметь:***

		поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности и соблюдает нормы здорового образа жизни;
		УК-7.5 ***Уметь:*** Применять здоровьесберегающие технологии для поддержания и обеспечения полноценной социальной и профессиональной деятельности
		УК-7.6 ***Уметь:*** использовать творчески средства и методы физического воспитания для профессионально-личностного развития, физического самосовершенствования, формирования здорового образа и стиля жизни
		УК-7.7 ***Владеть:*** Навыками использования здоровьесберегающих технологий в социальной и профессиональной деятельности
		УК-7.8 ***Владеть:*** Навыками выбора и эффективного применения здоровьесберегающих технологий в социальной и профессиональной деятельности
		УК-7.9 ***Владеть:*** навыками физического самосовершенствования, формирования здорового образа и стиля жизни
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 ***Знать***: Основы обеспечения безопасных и/или комфортных условий труда на рабочем месте, в т.ч. с помощью средств защиты;
		УК-8.2 ***Знать:*** Особенности и правила обеспечения безопасных и/или комфортных условий труда на рабочем месте, в т.ч. с помощью средств защиты;

		УК-8.3 ***Знать***: Правила действия в спасательных и неотложных аварийно-восстановительных мероприятиях в случае возникновения чрезвычайных ситуаций.
		УК-8.4 ***Уметь:*** Выявлять проблемы, связанные с нарушениями техники безопасности на рабочем месте;
		УК-8.5 ***Уметь:*** Выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте;
		УК-8.6 ***Уметь:*** Осуществлять действия по предотвращению возникновения чрезвычайных ситуаций (природного и техногенного происхождения) на рабочем месте, в т.ч. с помощью средств защиты
		УК-8.7 ***Владеть:*** Нывыками обеспечения безопасных и/или комфортных условий труда на рабочем месте, в т.ч. с помощью средств защиты;
		УК-8.8 ***Владеть:*** Способами выявления и устранения проблем, связанных с нарушениями техники безопасности на рабочем месте;
		УК-8.9 ***Владеть:*** Навыками участия в спасательных и неотложных аварийно-восстановительных мероприятиях в случае возникновения чрезвычайных ситуаций
Экономическая культура, в том числе финансовая грамотность	**УК-9.** Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1 Знать: базовые экономические понятия, объективные основы функционирования экономики и поведения экономических агентов;
		УК-9.2 Знать: принципы планирования экономической деятельности;

		условия функционирования национальной экономики; понятия и факторы экономического роста
		УК-9.3 Знать: основные документы, регламентирующие экономическую деятельность; источники финансирования профессиональной деятельности;
		УК-9.4 Уметь: использовать методы экономического планирования для достижения поставленных целей;
		УК-9.5 Уметь: анализировать экономическую и финансовую информацию, необходимую для принятия обоснованных решений в профессиональной сфере;
		УК-9.6 Уметь: обосновывать принятие экономических решений; принимать экономически обоснованные решения в конкретных ситуациях;
		УК-9.7 Владеть: навыками применения экономических инструментов;
		УК-9.8 Владеть: навыками планирования экономической деятельности;
		УК-9.9 Владеть: методами экономического и финансового планирования профессиональной деятельности
Гражданская позиция	**УК-10.** Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-10.1 Знать: природу экстремизма, терроризма, коррупции как социально-правового явления.
		УК-10.2 действующие уголовно-правовые нормы, обеспечивающие борьбу и противодействие экстремизму, терроризму и коррупционному поведению в различных областях жизнедеятельности.

		УК-10.3 способы профилактики и борьбы с проявлениями экстремизма и терроризма, коррупционного поведения и противодействия им в профессиональной деятельности, а также необходимость формирования нетерпимого отношения к ней
		УК-10.4 Уметь: проводить мероприятия, обеспечивающие формирование гражданской позиции и предотвращение коррупционного поведения в социуме, предотвращение проявлений экстремизма и терроризма
		УК-10.5 Уметь: планировать и организовывать мероприятия, обеспечивающие формирование гражданской позиции и предотвращение коррупционного поведения в социуме, предотвращение проявлений экстремизма и терроризма
		УК-10.6 Уметь: реализовывать средства обеспечения законности и правопорядка в сфере противодействия коррупционному поведению в социуме и предотвращения проявлений экстремизма и терроризма
		УК-10.7 Владеть: навыками взаимодействия в обществе на основе нетерпимого отношения к коррупционному поведению в социуме и предотвращения проявлений экстремизма и терроризма
		УК-10.8 Владеть: навыками организации работы в сфере профессиональной деятельности на основе нетерпимого отношения к коррупционному поведению, предотвращения проявлений экстремизма и терроризма

		УК-10.9 Владеть: навыками экспертно-консультативной работы по правовым вопросам противодействия коррупционному поведению, предотвращения проявлений экстремизма и терроризма
общепрофессиональные компетенции (ОПК)		
Наименование категории (группы) общепрофессиональны компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
	ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1. ***Знать:*** сущность и понятие информации, информационной безопасности и характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики;
		ОПК-1.2. ***Знать:*** источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
		ОПК-1.3. ***Знать:*** основные понятия, связанные с обеспечением информационной безопасности личности, общества и государства, понятия информационного противоборства, информационной войны и формы их проявлений в современном мире;
		ОПК-1.4. ***Уметь:*** классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

		ОПК-1.5. ***Уметь:*** классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
		ОПК-1.6. ***Уметь:*** применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
		ОПК-1.7. ***Владеть:*** профессиональной терминологией в области информационной безопасности
		ОПК-1.8. ***Владеть:*** основами языка программирования Python
		ОПК-1.9. ***Владеть:*** основами программирования на языках высокого уровня
	ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессионально й деятельности	ОПК-2.1. ***Знать:*** общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере; логико-математические основы построения электронных цифровых устройств; состав, назначение аппаратных средств и программного обеспечения персонального компьютера; элементы компьютерного дизайна и графического отображения объектов в виде чертежей или рисунков; типовые структуры и принципы организации компьютерных сетей назначение, функции и обобщённую структуру операционных систем назначение и основные компоненты систем баз данных; общие принципы построения, области и особенности применения языков программирования высокого уровня;

		ОПК-2.2. ***Знать:*** специализированные программные средства для моделирования режимов работы и исследования характеристик электрических цепей; основные возможности современных интегрированных сред разработки программного обеспечения на объектно-ориентированных языках программирования; возможности компиляторов программных проектов под различные операционные системы; наборы инструкций для системных утилит автоматической сборки программного обеспечения и установки программных пакетов объектно-ориентированных библиотек и фреймворков; методы коммутации и маршрутизации;
		ОПК-2.3. ***Знать:*** основные телекоммуникационные протоколы; принципы работы элементов и функциональных узлов современной электронной аппаратуры и физические процессы, протекающие в них; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; терминологию, основные руководящие и регламентирующие документы в области ЭВМ и вычислительных систем; характеристики программных разработок, позволяющих работать с алгебраическими структурами;
		ОПК-2.4. ***Уметь:*** применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети Интернет; составлять документы, используя прикладные программы офисного назначения; пользоваться средствами пользовательских интерфейсов операционных систем; применять методы построения компьютерных моделей изделий; применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной

		информационной сети Интернет; работать с интегрированной средой разработки программного обеспечения;
		ОПК-2.5. ***Уметь:*** использовать специализированные программные средства для моделирования режимов работы и исследования характеристик электрических цепей; использовать функциональные возможности современных интегрированных сред разработки программного обеспечения на объектно-ориентированных языках программирования для разработки прикладных программ; использовать утилиты автоматической сборки и развертывания программ в операционных системах; применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем выполнять расчеты, связанные с выбором режимов работы и определением оптимальных параметров радиооборудования и устройств цифрового тракта в составе СМС; анализировать статистические параметры трафика, проводить расчет интерфейсов внутренних направлений сети, изменять параметры коммутационной подсистемы, маршрутизации трафика, прописки кодов маршрутизации, анализировать статистику основных показателей эффективности радиосистем и систем передачи данных, выполнять расчет пропускной способности сетей радио и телекоммуникаций; применять программные средства моделирования функциональных узлов современной электронной аппаратуры;
		ОПК-2.6. ***Уметь:*** применять программные средства моделирования функциональных узлов современной электронной аппаратуры; применять стандартные программные

		средства для решения профессиональных задач; осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий; производить вычисления с помощью пакета GAP и аналогичных программных комплексов; осуществлять подготовку документов в среде типовых офисных пакетов
		ОПК-2.7. ***Владеть:*** навыком элементарного геометрического построения при помощи средств компьютерной графики; навыком построения двухмерных и трехмерных (3D) изображений изделий; проектирования, моделирования и анализа характеристик электрических цепей с помощью специализированных программных средств;
		ОПК-2.8. ***Владеть:*** навыками работы с основными современными интегрированными средами разработки программного обеспечения на объектно-ориентированных языках; разработки, отладки и развёртывания программного обеспечения в операционных системах семейства Windows и Linux; поиска и анализа возможностей современных интегрированных программных средств разработки прикладного программного обеспечения; проектирования сетей СМС различных стандартов и расчета их основных параметров в типовых ситуациях функционирования, работой на коммутационном оборудовании по обеспечению реализации новых услуг, сопровождения геоинформационных баз данных по сети радиодоступа, информационной поддержки расчетов радиопокрытия, радиорелейных и спутниковых трасс и частотно-территориального планирования в

		части использования картографической информации;
		ОПК-2.9. ***Владеть:*** навыками моделирования узлов современной электронной аппаратуры; использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры; программирования в пакете GAP
	ОПК-3. Способен использовать математические методы, необходимые для решения задач профессионально й деятельности	ОПК-3.1. ***Знать:*** основные понятия и задачи векторной алгебры и аналитической геометрии;***:*** основные свойства алгебраических структур; основы линейной алгебры над произвольными полями; основные понятия теории пределов и непрерывности функций одной и нескольких действительных переменных; основные методы дифференциального исчисления функций одной и нескольких действительных переменных; основные методы интегрального исчисления функций одной и нескольких действительных переменных;***:*** основные методы исследования числовых и функциональных рядов; основные задачи теории функций комплексного переменного;
		ОПК-3.2. ***Знать:*** основные типы обыкновенных дифференциальных уравнений и методы их решения; основные понятия, составляющие предмет теории поля, его дифференциальные и интегральные характеристики; основные понятия теории рядов; основные понятия и методы теории функций комплексного переменного; основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их основные свойства;***:*** классические предельные теоремы теории вероятностей;***:*** основные понятия теории случайных процессов; постановку задач и

		основные понятия математической статистики;
		ОПК-3.3. ***Знать:*** стандартные методы получения точечных и интервальных оценок параметров вероятностных распределений;***:*** стандартные методы проверки статистических гипотез; логику высказываний и предикатов; основы теории алгоритмов; свойства основных дискретных структур: конечных полей, графов, конечных автоматов, комбинаторных структур; основные понятия и методы теории графов; основные понятия и методы теории конечных автоматов; основные понятия и методы комбинаторного анализа; основные понятия и определения теории информации; определения и свойства основных алгебраических структур: групп, колец и полей; области применения основных моделей и методов построения искусственного интеллекта;
		ОПК-3.4. ***Уметь:*** строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач; решать основные задачи векторной алгебры и аналитической геометрии;***:*** решать основные задачи линейной алгебры, системы линейных уравнений над полями;***:*** использовать методы аналитической геометрии и векторной алгебры в смежных дисциплинах и физике;***:*** использовать методы линейной алгебры для решения прикладных задач; исследовать функциональные зависимости, возникающие для решения стандартных прикладных задач; использовать типовые модели и методы математического анализа для решения стандартных прикладных задач; проводить типовые расчеты с использованием основных формул дифференциального и интегрального исчисления;

		ОПК-3.5. ***Уметь:*** пользоваться справочными материалами по математическому анализу; применять методы теории поля, теории рядов, теории функций комплексного переменного для постановки и решения прикладных задач; применять стандартные вероятностные и статистические модели для решения типовых прикладных задач; пользоваться стандартными вероятностно-статистическими методами анализа экспериментальных данных; строить стандартные процедуры принятия решений на основе имеющихся экспериментальных данных; использовать расчетные формулы и таблицы для решения стандартных вероятностно-статистических задач; применять математические методы и вычислительную технику для решения практических задач; решать задачи периодичности и эквивалентности для конечных автоматов;
		ОПК-3.6. ***Уметь:*** применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач; решать оптимизационные задачи на графах; применять стандартные методы дискретной математики для решения профессиональных задач; решать типовые комбинаторные и теоретико-графовые задачи; использовать язык и средства дискретной математики для решения профессиональных задач; определять информационные характеристики системы передачи сообщений и каналов связи; производить вычисления в кольцах вычетов, матричных кольцах и в конечных полях; строить модели искусственного интеллекта для решения проектных задач, декомпозировать задачи на подзадачи и решать их с помощью методов искусственного интеллекта, интерпретировать полученные результаты;

		ОПК-3.7. ***Владеть:*** навыком решения задач, относящихся к теории поля, теории рядов и теории функций комплексного переменного; навыком применения изучаемого математического аппарата для решения прикладных задач;
		ОПК-3.8. ***Владеть:*** навыком применения методов математической логики и теории алгоритмов; навыком работы с элементами групп, колец и полей;
		ОПК-3.9. ***Владеть:*** навыком оформления технических заданий при решении задач с использованием методов искусственного интеллекта
	ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1. ***Знать:*** фундаментальные разделы физики; фундаментальные понятия и законы физики в области электростатики и электродинамики (закон Кулона, напряженность и потенциал электростатического поля, сила и плотность тока, законы Ома в интегральной и дифференциальной формах, закон Джоуля-Ленца, правила Кирхгофа, магнитное взаимодействие постоянных и переменных токов, закон Ампера, сила Лоренца, электромагнитная индукция, правило Ленца, явление самоиндукции индуктивность соленоида, емкость конденсатора); методы и средства измерения физических величин;***:*** методы обработки экспериментальныхданных; основные характеристики сигналов электросвязи, спектры и виды модуляции; эталонную модель взаимодействия открытых систем;
		ОПК-4.2. ***Знать:*** принципы построения и функционирования систем и сетей передачи информации; методы коммутации и маршрутизации;***:*** основные телекоммуникационные протоколы; принципы работы элементов и функциональных узлов современной электронной аппаратуры и физические процессы, протекающие в них;

		основы сертификации средств измерения и контроля, структуру и принципы работы измерительных устройств;
		ОПК-4.3. ***Знать:*** принципы функционирования радиотехнических систем и устройств; структуры типовых радиотехнических цепей и устройств, основные виды детерминированных сигналов в радиотехнике и методы их формирования и обработки; разложение в спектральный ряд по основным базисам (Фурье, Уолша, Котельникова и т. п.) и восстановление (синтез) сигнала по его спектру, а также погрешности синтеза; основные типы случайных процессов, их статистические и спектральные характеристики; основные типы нелинейных цепей, их модели и способы количественного описания характеристик; основы схемотехники современной радиоэлектронной аппаратуры;
		ОПК-4.4. ***Уметь:*** использовать знания фундаментальных основ, подходы и методы математики, физики в обучении и профессиональной деятельности, в интегрировании имеющихся знаний, наращивании накопленных знаний; применять математические методы, физические законы и вычислительную технику для решения практических задач; решать типовые задачи по следующим разделам курса физики: электростатика, электродинамика, постоянный и переменный ток, электромагнитная индукция; применять физические законы и вычислительную технику для решения практических задач; работать с измерительными приборами; выполнять физический эксперимент, обрабатывать результаты измерений, строить графики и проводить графический анализ опытных данных;
		ОПК-4.5.

		Уметь: проводить анализ показателей качества сетей и систем связи; анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи; проводить расчёты типовых аналоговых и цифровых узлов современной электронной аппаратуры; находить и определять область применения различных категорий и видов стандартов, систем стандартов, классификаторов и указателей, документацией продукции, процессов, услуг и систем качества; собирать измерительную схему;
		ОПК-4.6. ***Уметь:*** использовать спектральные и корреляционные методы анализа детерминированных и случайных сигналов при их передаче через радиотехнические цепи и устройства; иметь навыки получения и обработки осциллограмм и спектрограмм сигналов при экспериментах на физических и компьютерных моделях, уметь осуществлять синтез радиотехнических цепей и сигналов по различным критериям; применять на практике методы анализа электрических цепей; осуществлять синтез структурных и электрических схем электронных устройств; использовать стандартные методы и средства проектирования электронных узлов и устройств, в том числе для средств защиты информации;
		ОПК-4.7. ***Владеть:*** навыком организации, планирования, проведения и обработки результатов экспериментов и экспериментальных исследований; навыком работы с измерительной аппаратурой, в том числе с цифровой измерительной техникой; навыком обработки экспериментальных данных и оценки точности измерений; навыком анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации;

		ОПК-4.8. ***Владеть:*** навыком использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; навыком работы с современной элементной базой электронной аппаратуры; навыком использования различных категорий и видов стандартов, систем стандартов, классификаторов и указателей, документацией продукции, процессов, услуг и систем качества;
		ОПК-4.9. ***Владеть:*** навыком использования различных средств измерения; навыком самостоятельной работы с учебной и справочной литературой по радиотехнике, получения и обработки осциллограмм , спектрограмм и других характеристик сигналов при экспериментах на физических и компьютерных моделях; навыком методами расчета типовых электронных устройств, навыками чтения принципиальных схем, навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы;
	ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1. ***Знать:*** основы правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации; основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; правовые основы организации защиты государственной тайны и конфиденциальной информации,

		правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации;
		ОПК-5.2. ***Знать:*** статус и порядок работы основных правовых информационно-справочных систем; основы организации и деятельности органов государственной власти в Российской Федерации; основные документы по стандартизации в сфере управления ИБ; принципы формирования политики информационной безопасности в автоматизированных системах;
		ОПК-5.3. ***Знать:*** требования информационной безопасности при эксплуатации автоматизированной системы; требования нормативных документов к составу, содержанию и оформлению технической документации объекта информатизации; виды и состав документации современной организации, особенности документирования профессиональной деятельности;
		ОПК-5.4. ***Уметь:*** применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и

		аттестации по требованиям безопасности информации;
		ОПК-5.5. ***Уметь:*** формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; формировать политики информационной безопасности организации;
		ОПК-5.6. ***Уметь:*** выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы; разрабатывать техническую документацию объекта информатизации; определять виды документов, необходимых для оформления управленческих действий в профессиональной деятельности, грамотно составлять и оформлять служебные документы;
		ОПК-5.7. ***Владеть:*** понятийно-категориальным аппаратом юриспруденции; навыками установления фактических обстоятельств, юридической основы и квалификации;
		ОПК-5.8. ***Владеть:*** навыком работы с нормативными правовыми актами различной юридической силы; навыками применения основных законов, связанных с организационно-правовым обеспечением информационной безопасности в профессиональной деятельности;
		ОПК-5.9. ***Владеть:*** навыками организации и обеспечения режима секретности; методами организации и управления служб защиты информации на предприятии;

		методами формирования требований по защите информации
	ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1. ***Знать:*** систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации; систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации;
		ОПК-6.2. ***Знать:*** задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
		ОПК-6.3. ***Знать:*** принципы формирования комплекса мер по защите информации ограниченного доступа объектов информатизации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
		ОПК-6.4. ***Уметь:*** классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; засекречивать и рассекречивать сведения и их носители;
		ОПК-6.5. ***Уметь:*** использовать систему организационных мер, направленных на защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими

		документами ФСБ России, ФСТЭК России; определять комплекс мер для обеспечения защиты информации объектов информатизации;
		ОПК-6.6. ***Уметь:*** применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
		ОПК-6.7. ***Владеть:*** навыком анализа информационной инфраструктуры информационной системы и ее безопасности объектов информатизации; навыками применения основных законов, связанных с организационно-правовым обеспечением информационной безопасности в профессиональной деятельности;
		ОПК-6.8. ***Владеть:*** навыками работы с нормативными правовыми актами; навыками организации и обеспечения режима секретности;
		ОПК-6.9. ***Владеть:*** методами организации и управления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации;
	ОПК-7. Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ОПК-7.1. ***Знать:*** ключевые понятия и особенности разработки программных средств для решения задач профессиональной деятельности с использованием объектно-ориентированного подхода; язык программирования высокого уровня (основы объектно-ориентированного программирования); стандартные алгоритмы и методы организации и обработки данных; методы

		разработки алгоритмов и программ в рамках объектно-ориентированной парадигмы программирования на современном языке высокого уровня; принципы объектно-ориентированной парадигмы: абстрагирование, инкапсуляция, наследование, полиморфизм;
		ОПК-7.2. ***Знать:*** основные синтаксические конструкции объектно-ориентированного языка программирования: классы, поля, свойства, методы, выражения, события; методы обобщенного программирования; методы оценки сложности алгоритмов; функциональные возможности стандартной библиотеки языка и фреймворка; современные технологии и методы программирования;
		ОПК-7.3. ***Знать:*** принципы организации документирования разработки, процесса сопровождения программного обеспечения; основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико-графовые алгоритмы; показатели качества программного обеспечения; базовые принципы сбора информации для обработки и анализа при помощи методов машинного обучения с учетом современных тенденций развития электроники, измерительной и вычислительной техники и информационных технологий; базовые принципы сбора информации для обработки и анализа при помощи методов искусственного интеллекта с учетом современных тенденций развития электроники, измерительной и вычислительной техники и информационных технологий;
		ОПК-7.4. ***Уметь:*** использовать технологии разработки программных средств для решения задач профессиональной деятельности; разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых

		профессиональных задач; разрабатывать алгоритмы и программы в рамках объектно-ориентированной парадигмы на современном языке программирования высокого уровня с применением основных синтаксических конструкций и функциональных возможностей стандартной библиотеки языка и фреймворка;
		ОПК-7.5. ***Уметь:*** проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач;
		ОПК-7.6. ***Уметь:*** модернизировать и адаптировать стандартные методы машинного обучения с учетом современных тенденций развития электроники, измерительной и вычислительной техники и информационных технологий; модернизировать и адаптировать стандартные методы искусственного интеллекта с учетом современных тенденций развития электроники, измерительной и вычислительной техники и информационных технологий
		ОПК-7.7. ***Владеть:*** навыками программирования элементов информационных систем, требующие объектно-ориентированного подхода; навыками разработки алгоритмов и программ;
		ОПК-7.8. ***Владеть:*** навыками отладки, поиска и устранения ошибок программного кода; навыком оценки сложности алгоритмов; навыками использования возможностей стандартной библиотеки, сторонних библиотек программного кода и фреймворков;

		ОПК-7.9. ***Владеть:*** навыком разработки и модернизации методов машинного обучения с учетом современных тенденций развития электроники, измерительной и вычислительной техники и информационных технологий; навыками разработки и модернизации методов искусственного интеллекта с учетом современных тенденций развития электроники, измерительной и вычислительной техники и информационных технологий;
	ОПК-8. Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	ОПК-8.1. ***Знать:*** методы и средства измерения физических величин;
		ОПК-8.2. ***Знать:*** методы обработки экспериментальных данных;
		ОПК-8.3. ***Знать:*** цели, задачи и основные методы научных исследований при решении задач профессиональной деятельности
		ОПК-8.4. ***Уметь:*** работать с измерительными приборами; выполнять физический эксперимент, обрабатывать результаты измерений, строить графики и проводить графический анализ опытных данных;
		ОПК-8.5. ***Уметь:*** считать систематические и случайные ошибки прямых и косвенных измерений, приборные ошибки; применять современное физическое оборудование и приборы при решении практических задач;
		ОПК-8.6. ***Уметь:*** использовать стандартные вероятностно-статистические методы анализа экспериментальных данных; обобщать, анализировать и систематизировать научную информацию в области информационной безопасности;
		ОПК-8.7 ***Владеть:*** навыками организации, планирования, проведения и обработки результатов экспериментов и

		экспериментальных исследований; навыками проведения физического эксперимента и умения применять конкретное физическое содержание в прикладных задачах будущей специальности;
		ОПК-8.8. ***Владеть:*** навыками проведения расчетов, как при решении задач, так и при научном эксперименте; навыком оформления отчетов по результатам исследований;
		ОПК-8.9. ***Владеть:*** навыками подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;
	ОПК-9. Способен решать задачи профессионально й деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.1. ***Знать:*** основные положения стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД); типовые методики проведения измерений параметров, характеризующих наличие технических каналов утечки информации; принципы организации информационных систем в соответствии с требованиями по защите информации; особенности комплексного подхода к обеспечению информационной безопасности организации;
		ОПК-9.2. ***Знать:*** программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; базовые понятия и определения киберфизической системы, базовые принципы теории управления системами, формирования целей, методов и критериев качества управления, формализованных стратегий основы, понятия и определения информационно-управляющих систем;
		ОПК-9.3. ***Знать:*** основы теории сетевой организации информационно-

		вычислительных распределенных систем и компьютерных сетей, архитектуры и иерархии сетевой организации; основы модели знаний, базовые понятия теории формирования баз данных и баз знаний; подходы к построению платформы киберфизической системы как гибридной сетевой среды с интегрированными вычислительными и физическими возможностями
		ОПК-9.4. ***Уметь:*** применять требования стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД); проводить контрольно-измерительные работы в целях оценки количественных характеристик технических каналов утечки информации; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
		ОПК-9.5. ***Уметь:*** разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности; анализировать подходы к построению гибридной информационно-управляющей среды, ориентированной на решение широкого класса прикладных задач, в том числе связанных с обеспечением информационной безопасности;
		ОПК-9.6. ***Уметь:*** ставить задачи формирования архитектуры, принципов построения и функционирования киберфизической системы; ставить задачи проведение аналитики киберугроз и оценки уязвимостей и рисков киберфизической системы
		ОПК-9.7.

		Владеть: навыками разработки технической документации в соответствии с требованиями стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД);т навыками использования современных сетевых технологий;
		ОПК-9.8. ***Владеть:*** навыками проектирования системы защиты объекта информатизации от утечек информации за счет несанкционированного доступа; навыками анализа основных характеристик и возможностей телекоммуникационных систем по передачи информации;
		ОПК-9.9. ***Владеть:*** методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; навыками применения полученных знаний на практике;
	ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1. ***Знать:*** основные понятия и задачи криптографии, математические модели криптографических систем; основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы;
		ОПК-10.2. ***Знать:*** национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения;***:*** предназначение криптографических протоколов в реализации политик информационной безопасности;
		ОПК-10.3. ***Знать:*** область применения криптографических протоколов в

		системе защиты автоматизированных систем;
		ОПК-10.4. ***Уметь:*** использовать систему криптографической защиты информации (СКЗИ) для решения задач профессиональной деятельности;
		ОПК-10.5. ***Уметь:*** производить вычисления в алгебраических структурах (группах, кольцах и полях); применять теоретико-графовые и теоретико- множественные методы при реализации протоколов;
		ОПК-10.6. ***Уметь:*** производить аудит результатов выполненного протокола;
		ОПК-10.7. ***Владеть:*** криптографической терминологией;
		ОПК-10.8. ***Владеть:*** навыками применения криптографических протоколов при решении задач профессиональной деятельности;
		ОПК-10.9. ***Владеть:*** навыками применять изучаемый математический аппарат для исследования свойств криптографических преобразований;
	ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ОПК-11.1. ***Знать:*** основные понятия теории информации и кодирования; принципы, методы и средства выявления угроз безопасности автоматизированных систем; принципы аутентификации и идентификации пользователей; концепцию построения системы разграничения доступа; основные меры по защите информации в автоматизированных системах;
		ОПК-11.2. ***Знать:*** содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем;

		особенности межсетевого экранирования;
		ОПК-11.3. ***Знать:*** программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях
		ОПК-11.4. ***Уметь:*** выявлять и уничтожать компьютерные вирусы; работать со специальной технической литературой; использовать электронные цифровые подписи; противодействовать нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
		ОПК-11.5. ***Уметь:*** проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы;
		ОПК-11.6. ***Уметь:*** проектировать информационные системы; обосновывать и планировать состав и архитектуру моделируемых и проектируемых информационных, автоматизированных и автоматических систем; разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности; настраивать программное обеспечение системы защиты информации автоматизированной системы;
		ОПК-11.7. ***Владеть:*** навыками эксплуатации и обслуживания аппретуры, оборудования и программного

		обеспечения, связанных с обеспечением безопасности информации; навыками шифрования и защиты от несанкционированного доступа;
		ОПК-11.8. ***Владеть:*** навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;
		ОПК-11.9. ***Владеть:*** навыками участия в разработке системы обеспечения информационной безопасности объекта; навыками проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности;
	ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12.1. ***Знать:*** методы проектирования вычислительных сетей;
		ОПК-12.2. ***Знать:*** устройство и принципы работы операционных систем, структуру и возможности подсистем защиты операционных систем семейств UNIX и Windows;
		ОПК-12.3. ***Знать:*** назначение, функции и структуру систем управления базами данных;
		ОПК-12.4. ***Уметь:*** проектировать вычислительные сети; использовать средства управления работой операционной системы; формулировать политику безопасности операционных систем семейств UNIX и Windows;
		ОПК-12.5. ***Уметь:*** эксплуатировать базы данных; создавать объекты базы данных;
		ОПК-12.6 ***Уметь:*** выполнять запросы к базе данных; разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных;

		ОПК-12.7. ***Владеть:*** навыками эксплуатации локальных вычислительных сетей;
		ОПК-12.8. ***Владеть:*** навыками установки операционных систем семейств Windows и Unix;
		ОПК-12.9. ***Владеть:*** навыком эксплуатации баз данных с учетом требований по обеспечению информационной безопасности;
	ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ОПК-13.1. ***Знать:*** риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки; организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы; классификацию и количественные характеристики технических каналов утечки информации;
		ОПК-13.2. ***Знать:*** способы и средства защиты информации от утечки по техническим каналам, контроля их эффективности; организацию защиты информации от утечки по техническим каналам на объектах информатизации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по обеспечению безопасности информации в автоматизированных системах;
		ОПК-13.3. ***Знать:*** способы обеспечения контроля безопасности автоматизированных систем; основные информационные технологии, используемые в автоматизированных системах; методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;
		ОПК-13.4. ***Уметь:*** анализировать и оценивать угрозы информационной безопасности автоматизированных систем;

		осуществлять управление и администрирование защищенных автоматизированных систем;
		ОПК-13.5. ***Уметь:*** разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; использовать средства инструментального контроля показателей эффективности технической защиты информации;
		ОПК-13.6. ***Уметь:*** осуществлять планирование, организацию и контроль над безопасностью автоматизированной системы с учетом требований по защите информации; восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях;
		ОПК-13.7. ***Владеть:*** навыками анализа информационной инфраструктуры автоматизированных систем; навыками разработки политик информационной безопасности автоматизированных систем;
		ОПК-13.8. ***Владеть:*** навыками проектирования системы защиты объекта информатизации от утечек по техническим каналам; навыками применения способов обеспечения контроля безопасности автоматизированных систем;
		ОПК-13.9. ***Владеть:*** навыками разработки документов для обеспечения контроля безопасности информации в автоматизированной системе при её эксплуатации (включая управление инцидентами информационной безопасности); навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;
	ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию	ОПК-14.1. ***Знать:*** основы построения, расчета и анализа современной

	автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	системы показателей, характеризующих деятельность хозяйствующих субъектов на микроуровне; критерии оценки защищенности автоматизированной системы; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
		ОПК-14.2. ***Знать:*** регламент проведения аттестационных испытаний; требования защиты информации к аттестованным объектам;
		ОПК-14.3. ***Знать:*** требования к этапам ввода и вывода из эксплуатации системы защиты информации; организационные, правовые, программно-аппаратные, криптографические, технические меры по защите информации, реализуемые в автоматизированных системах;
		ОПК-14.4. ***Уметь:*** осуществлять расчет себестоимости продукции; рассчитывать влияние факторов на различные виды расходов; осуществлять расчет потребности в инвестициях;
		ОПК-14.5 ***Уметь:*** контролировать уровень защищенности в автоматизированных системах; разрабатывать программу и методики аттестационных испытаний;
		ОПК-14.6. ***Уметь:*** разрабатывать заключение по результатам аттестационных испытаний; администрировать подсистемы информационной безопасности автоматизированных систем;
		ОПК-14.7. ***Владеть:*** владения методами распределения накладных затрат и оценки эффективности проектных решений; анализа событий, связанных с защитой информации в автоматизированных системах;
		ОПК-14.8. ***Владеть:*** навыками проведения аттестационных испытаний; мониторинга изменения состояния

		аттестованного объекта информатизации;
		ОПК-14.19. ***Владеть:*** использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;
	ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1. ***Знать:*** методы администрирования вычислительных сетей; методы администрирования и принципы работы операционных систем семейств UNIX и Windows; принципы формирования политики информационной безопасности в автоматизированных системах; методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы;
		ОПК-15.2. ***Знать:*** средства обеспечения безопасности данных; основные угрозы безопасности информации и модели нарушителя объекта информатизации; цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью; принципы формирования политики информационной безопасности объекта информатизации;
		ОПК-15.3. ***Знать:*** методы и средства контроля защищенности объектов информатизации; узлы автоматизированной системы для измерения параметров информативных сигналов технических средств обработки информации; измерительную аппаратуру, применяемую для контроля защищенности объектов информатизации;
		ОПК-15.4. ***Уметь:*** администрировать вычислительные сети; реализовывать политику безопасности вычислительной

		сети; настраивать политику безопасности операционных систем семейств UNIX и Windows; разрабатывать частные политики информационной безопасности автоматизированных систем;
		ОПК-15.5. ***Уметь:*** осуществлять диагностику и мониторинг систем защиты автоматизированных систем; администрировать базы данных; разрабатывать модели угроз и модели нарушителя объекта информатизации;
		ОПК-15.6. ***Уметь:*** оценивать информационные риски объекта информатизации; разрабатывать порядок проведения измерений параметров информативных сигналов технических средств обработки информации; обрабатывать и интерпретировать результаты измерений параметров информативных сигналов технических средств обработки информации;
		ОПК-15.7. ***Владеть:*** навыками администрирования локальных вычислительных сетей с учетом требований по обеспечению информационной безопасности; навыками администрирования операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности; навыками управления процессами обеспечения безопасности автоматизированных систем;
		ОПК-15.8. ***Владеть:*** навыками администрирования баз данных с учетом требований по обеспечению информационной безопасности; навыками эксплуатации измерительной аппаратуры контроля защищенности объектов информатизации с учетом требований по обеспечению информационной безопасности;
		ОПК-15.9. ***Владеть:*** навыками применения методов математической обработки результатов измерений

		параметров информативных сигналов технических средств обработки информации; навыками экспертизы состояния защищенности информации на объектах информатизации
	ОПК-16. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	ОПК-16.1. ***Знать:*** периодизацию, основные факты, явления и процессы всемирной и отечественной истории
		ОПК-16.2. ***Знать:*** периодизацию, основные факты, явления и процессы всемирной и отечественной истории; особенности исторического пути России, ее место и роль в мировом сообществе в контексте всеобщей истории
		ОПК-16.3. ***Знать:*** основные этапы и закономерности исторического развития России, в том числе для формирования гражданской позиции и развития патриотизма
		ОПК-16.4. ***Уметь:*** анализировать основные этапы и закономерности исторического развития России, в том числе для формирования гражданской позиции и развития патриотизма;
		ОПК-16.5. ***Уметь:*** сравнивать и осмысливать национальные идеи и ценности разных стран и народов; разоблачать мифы о русской истории, характере и ценностях россиян;
		ОПК-16.6. ***Уметь:*** формулировать национальные интересы в эпоху глобализма; аргументировать гражданскую позицию по ключевым историческим событиям российской истории и современной социально-политической ситуации;
		ОПК-16.7.

		Владеть: навыком анализа основных этапов и закономерностей исторического развития России, в том числе для формирования гражданской позиции и развития патриотизма
		ОПК-16.8. ***Владеть:*** технологией логических рассуждений, умозаключений и выводов;
		ОПК-16.9. ***Владеть:*** технологией аргументации защиты национальных ценностей;
	ОПК-11.1. Способен планировать и разрабатывать меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры	ОПК-11.1. ***Знать:*** требования нормативных правовых актов в области защиты информации значимых объектов критической информационной инфраструктуры; основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами значимых объектов критической информационной инфраструктуры;
		ОПК-11.2. ***Знать:*** основы взаимодействия субъектов критической информационной инфраструктуры с ФСТЭК России, ФСБ России, ГосСОПКа; методику формирования моделей нарушителей и методику оценки угроз безопасности информации значимых объектов критической информационной инфраструктуры
		ОПК-11.3. ***Знать:*** задачи и полномочия подразделения по защите информации; основы построения систем безопасности значимых объектов критической информационной инфраструктуры и обеспечения их функционирования; процедуру категорирования объектов критической информационной

		инфраструктуры, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости; форму направления в ФСТЭК России сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо отсутствии необходимости присвоения ему одной из таких категорий; общие требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры; методы и средства обеспечения безопасности значимых объектов критической информационной инфраструктуры
		ОПК-11.4. ***Уметь:*** проводить анализ исходных данных и проектных решений при разработке подсистем и средств обеспечения безопасности значимых объектов критической информационной инфраструктуры
		ОПК-11.5. ***Уметь:*** определять источники угроз безопасности информации и проводить оценку возможностей нарушителей по реализации угроз безопасности информации
		ОПК-11.6. ***Уметь:*** планировать и разрабатывать организационно-правовые и программно-технические меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры
		ОПК-11.7. ***Владеть:*** навыками работы с нормативными правовыми актами, методическими документами в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;
		ОПК-11.8.

		Владеть: навыками разработки организационно-распорядительных документов по безопасности значимых объектов критической информационной инфраструктуры; навыками определения комплекса мер для защиты информации значимых объектов критической информационной инфраструктуры;
		ОПК-11.9. ***Владеть:*** внедрения организационных и технических мер по обеспечению безопасности значимого объекта критической информационной инфраструктуры; навыком : проектирования подсистем безопасности значимых объектов критической информационной инфраструктуры
	ОПК-11.2. Способен обеспечивать функционирование систем безопасности значимых объектов критической информационной инфраструктуры	ОПК-11.1. **Знать**: требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры
		ОПК-11.2. ***Знать:*** программно-аппаратные средства защиты информации, входящие в состав систем безопасности значимых объектов критической информационной инфраструктуры
		ОПК-11.3. ***Знать:*** способы и методы эксплуатации автоматизированных систем в защищенном исполнении при обеспечении безопасности значимых объектов критической информационной инфраструктуры
		ОПК-11.4. ***Уметь:*** обеспечивать реализацию требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленных в соответствии со статьей 11 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»
		ОПК-11.5. ***Уметь:*** обеспечивать в соответствии с требованиями по безопасности реализацию

		организационных мер и эксплуатацию средств защиты информации
		ОПК-11.6. ***Уметь:*** готовить предложения по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов критической информационной инфраструктуры
		ОПК-11.7. ***Владеть:*** навыком технической эксплуатации средств защиты информации при обеспечении безопасности значимых объектов критической информационной инфраструктуры; навыками установки, настройки и использования программных средств системного и прикладного назначения, управления программных обеспечением;
		ОПК-11.8. ***Владеть:*** навыками работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов критической информационной инфраструктуры, в том числе зарубежными информационными ресурсами;
		ОПК-11.9. ***Владеть:*** навыками планирования мероприятий по обеспечению безопасности значимого объекта критической информационной инфраструктуры;
	ОПК-11.3. Способен организовывать и осуществлять меры по контролю состояния безопасности значимых объектов критической информационной инфраструктуры	ОПК-11.1. ***Знать:*** методику проведения аудита информационной безопасности значимых объектов критической информационной инфраструктуры
		ОПК-11.2. ***Знать:*** способы выявления уязвимостей в операционных системах средств вычислительной техники и телекоммуникационного оборудования значимых объектов

		критической информационной инфраструктуры
		ОПК-11.3. ***Знать:*** организационные и технические основы построения систем безопасности значимых объектов критической информационной инфраструктуры и обеспечения их функционирования;
		ОПК-11.4. ***Уметь:*** организовывать проведение оценки соответствия значимых объектов критической информационной инфраструктуры требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленных в соответствии со статьей 11 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»
		ОПК-11.5. ***Уметь:*** проводить инвентаризацию систем и сетей, анализ уязвимостей, тестирование на проникновение систем и сетей с использованием соответствующих автоматизированных средств; проводить оценку уровня защищенности (аудит) систем и сетей и содержащейся в них информации
		ОПК-11.6. ***Уметь:*** проводить документирование процедур и результатов контроля за обеспечением безопасности значимого объекта
		ОПК-11.7. ***Владеть:*** навыком проведения контроля (анализа) защищенности значимого объекта с учетом особенностей его функционирования

			ОПК-11.8. ***Владеть:*** навыками анализа угроз безопасности информации в значимом объекте критической информационной инфраструктуры и последствий от их реализации; навыками управления (администрирования) подсистемой безопасности значимого объекта критической информационной инфраструктуры; навыками реагирования на компьютерные инциденты в ходе эксплуатации значимого объекта критической информационной инфраструктуры(	
			ОПК-11.9. ***Владеть:*** навыками обеспечения действий в нештатных ситуациях в ходе эксплуатации значимого объекта критической информационной инфраструктуры; информирования и обучения персонала значимого объекта критической информационной инфраструктуры; навыками контроля за обеспечением безопасности значимого объекта критической информационной инфраструктуры; оценки возможных последствий реализации угроз безопасности информации в значимом объекте критической информационной инфраструктуры;	
профессиональные компетенции ПК				
Задача профессиональной деятельности	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС, анализ опыта)
тип задач профессиональной деятельности - **научно-исследовательский**				
01 Образование и наука (в сфере научных исследований); 06 Связь,	Обеспечение защиты информации в автоматизированных системах,	**ПК-1**. Способен моделировать защищенные автоматизированные	ПК-1.1. ***Знать:*** методы проведения физических исследований, технические и	на основе обобщения отечественного и зарубежного опыта,

информационные и коммуникационные технологии (в сфере обеспечения безопасности информации в автоматизированных системах); 12 Обеспечение безопасности (в сфере обеспечения безопасности информации в автоматизированных системах, обладающих информационно-технологическими ресурсами, подлежащими защите); сфера обороны и безопасности; сфера правоохранительной деятельности.	используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации Разработка систем защиты информации автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых	системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	программные средства, применяемые при анализе электромагнитных полей и волн; уравнения и законы электродинамики и распространения радиоволн; модели элементарных излучателей; основные типы антенн, применяемых при анализе электромагнитных полей; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; ПК-1.2. ***Знать:*** назначение, функции и структуру информационных и библиографических систем; методы поиска, изучения и обобщения научно-технической литературы, нормативных и методических материалов; основные методы исследования по теме своей научно-исследовательской работы; основы	проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники, с учетом мнения экспертов из числа представителей заинтересованных организаций и иных источников

	отсутствует необходимость присвоения им категорий значимости		теории цифровой обработки сигналов как теоретической базы для разработки и исследования методов обработки, приема и передачи данных в системах обеспечения информационной безопасности автоматизированных систем управления; актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности; цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и виды АСУ	
			ПК-1.3. ***Знать:*** состав автоматизированных систем управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и уровни управления АСУ	

			ТП, место АСУ ТП в интегрированных системах управления; области задач организации информационных технологий и современные инструменты построения интеллектуальных систем, обеспечивающих информационную безопасность; основные принципы и проблематику теории обучения машин, основные современные методы обучении по прецедентам — классификации, кластеризации и регрессии; принципы организации информационных систем в соответствии с требованиями по защите информации; основные способы кодирования информации в автоматизированных системах управления (АСУ), обеспечивающие максимальную надежность и высокую скорость при ее передаче по каналам связи (коды: линейные, циклические, БЧХ, Хэмминга, Шеннона - Фано и Хаффмана); уязвимости	

			современных АСУ ТП, подходы к устранению уязвимостей и построению системы защиты современных АСУ ТП; основные виды математических моделей информационных потоков и систем защиты информации и методы их построения	
			ПК-1.4. ***Уметь:*** использовать методы проведения физических исследований, технические и программные средства для анализа электромагнитных полей технических средств автоматизированных систем; использовать методы исследования электромагнитных полей для оценки физических характеристик технических средств автоматизированных систем; определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; определять методы управления	

			доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе; определять параметры информационной системы и ее структуру в соответствии с заданными функциями;	
			ПК-1.5. ***Уметь:*** составлять обзоры по вопросам обеспечения информационной безопасности по теме своей научно-исследовательской работы; применять методы исследования по теме своей научно-исследовательской работы; формировать математическое описание дискретных систем в виде алгоритмов; выполнять компьютерное моделирование дискретных систем на основе их математического описания; анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах	

			автоматизации; анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации; формулировать основные задачи, возникающие при анализе данных, пути их решения, выбирать адекватные алгоритмы решения задачи анализа данных, оценивать качество получаемых решений, обеспечивающих информационную безопасность;	
			ПК-1.6. ***Уметь:*** формализовать постановки прикладных задач анализа данных, применять основные методы создания алгоритмов интеллектуального анализа данных в системах информационной безопасности, такие как классификация, кластеризация и прогнозирование; оценивать информационные риски в информационных системах; решать типовые задачи кодирования и декодирования информации с использованием математических методов и	

			моделей; анализировать структуры АСУ ТП, строить их модели, оценивать риски функциональной безопасности, распознавать атаки социальной инженерии; на основе опытных данных и технических характеристик автоматизированной системы управления (АСУ) строить адекватную математическую модель, связанную с системой защиты информации в АСУ	
			ПК-1.7. ***Владеть:*** навыком применения методик исследования электромагнитных полей; навыком применения исследовательских методов электродинамики и распространения радиоволн; навыками поиска и изучения научно-технической литературы, а также изложения и оформления результатов своей научно-исследовательской работы; навыком составления математических моделей дискретных	

			систем и сигналов;	
			ПК-1.8. ***Владеть:*** навыком разработки алгоритмов цифровой обработки сигналов в системах информационной безопасности; навыком выбора методов проведения и обработки экспериментальных исследований, оформления научно-технических отчётов, обзоров, докладов, статей; навыком выбора и обоснованием критериев эффективности функционирования защищенных информационных систем	
			ПК-1.9. ***Владеть:*** навыком применения помехоустойчивых шифров и кодов, повышающих скорость передачи информации в АСУ; навыком разработки политик безопасности современных промышленных систем автоматизации, исследования сетевых пакетов в промышленной сети; навыком применения	

			математических моделей для построения системы защиты информации в АСУ и оценки ее эффективности	
	тип задач профессиональной деятельности - **проектный**			
	Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации Разработка систем защиты информации автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости	**ПК-2.** Способен разрабатывать проектные решения по защите информации в автоматизированных системах	ПК-2.1. ***Знать:*** основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; основные алгоритмы при цифровой обработке сигналов, факторы, определяющие связь эксплуатационных свойств систем цифровой обработки сигналов с их техническими характеристиками и; цели и задачи проектирования систем инженерно-технической защиты объектов; основные понятия и терминологию, принятые в проектировании систем инженерно-технической защиты объектов	
			ПК-2.2. ***Знать:*** основные	

	Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости		принципы проектирования систем инженерно-технической защиты объектов; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; основные методы создания алгоритмов интеллектуального анализа данных в системах информационной безопасности, такие как классификация, кластеризация и прогнозирование	
			ПК-2.3. ***Знать:*** базовые алгоритмы анализа данных: k-средних, метод опорных векторов, линейная регрессия, ассоциативные правила, деревья решений, анализ выбросов или анализ аномалий, искусственные нейронные сети; меры, операции и приемы, направленные на предотвращение утечки защищаемой информации, несанкционированного и	

			непреднамеренного воздействия на защищаемую информацию в сферах федерального, регионального управления и электронной коммерции; основные этапы реализации проектных решений в области автоматизированных систем электронного документооборота	
			ПК-2.4. ***Уметь:*** определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы; обоснованно оценивать необходимые параметры дискретизации и квантования, интерполяции и децимации сигналов; объяснять принцип методов оценки параметров сигналов, используемых в системах обеспечения информационной безопасности автоматизированных систем управления; изучать научно-техническую информацию, отечественный и зарубежный опыт	

			и организовывать работы по практическому использованию новых технологий в области цифровой обработки сигналов	
			ПК-2.5. ***Уметь:*** проводить анализ вероятных угроз охраняемому объекту; выбирать наиболее рациональные методы противодействия угрозам охраняемому объекту; выбирать технические средства для решения задачи охраны объекта; определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации; реализовывать в виде программного кода базовые алгоритмы анализа данных: k- средних, метод опорных векторов, линейная регрессия, ассоциативные правила, искусственные нейронные сети	

			ПК-2.6. ***Уметь:*** способы построения систем с нечеткой логикой; изучать научно-техническую информацию, отечественный и зарубежный опыт и организовывать работы по практическому использованию новых технологий в области интеллектуального анализа данных; вырабатывать и принимать организационно-технические решения, адекватные степени угроз, в различных отраслях деятельности; разрабатывать защищенные системы электронного документооборота	
			ПК-2.7. ***Владеть:*** навыком применения типовых прикладных пакетов для синтеза алгоритмов цифровой обработки сигналов, используемых в системах обеспечения информационной безопасности автоматизированных систем	

			управления; навыком разработки проектов нормативных документов, регламентирующих их работу по защите информации	
			ПК-2.8. ***Владеть:*** навыком разработки алгоритмов интеллектуального анализа данных в системах информационной безопасности; навыком разработки предложений по совершенствованию систем информационной безопасности предприятий и организаций, комплексно обеспечивающих повышение ее уровня	
			ПК-2.9. ***Владеть:*** навыком разработки и анализом проектных решений в области автоматизированных систем электронного документооборота	
	тип задач профессиональной деятельности - **контрольно-аналитический**			
	Обеспечение защиты	**ПК-3.**	ПК-3.1. ***Знать:*** архитектуру	

	информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации Разработка систем защиты информации автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной	Способен выполнять работы по мониторингу и аудиту защищенности информации в автоматизированных системах	промышленных сетей АСУ ТП; физические принципы, на которых строятся системы инженерно-технической защиты объектов; типы современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП	
			ПК-3.2. ***Знать:*** средства и меры информационной безопасности, применяемые в промышленных и корпоративных системах автоматизации; основные понятия мониторинга событий, методы сбора информации о событиях, принципы работы систем управления информацией и событиями в безопасности SIEM	
			ПК-3.3. ***Знать:*** принципы работы систем мониторинга информационной безопасности автоматизированных систем;	

	инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости		методы и средства обеспечения информационной безопасности в системах электронного документооборота	
			ПК-3.4. ***Уметь:*** применять методы и средства регистрации, записи и хранения значимых параметров потоков данных АСУ ТП; проводить оптимизацию структуры комплексов инженерно-технической защиты объектов	
			ПК-3.5. ***Уметь:*** проводить аналитику современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП; использовать средства сбора и анализа информации о событиях информационной безопасности для целей мониторинга	

			информационной безопасности	
			ПК-3.6. ***Уметь:*** формировать правила анализа событий мониторинга информационной безопасности автоматизированных систем; определять необходимые методы и средства обеспечения информационной безопасности в системах электронного документооборота	
			ПК-3.7. ***Владеть:*** навыком определения ключевых точек мониторинга значимых параметров потоков данных, распределенных в информационной системе промышленных сетей АСУ ТП; навыком анализа критериев оценки параметров технических средств охраны объектов	
			ПК-3.8. ***Владеть:*** навыком составления программы испытаний систем инженерно-технической защиты объектов;	

			навыком оценки уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП	
			ПК-3.9. ***Владеть:*** навыком использования методов мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; навыком проведения контрольных проверок работоспособности и и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	
	тип задач профессиональной деятельности - **организационно-управленческий**			
	Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых	**ПК-4.** Способен разрабатывать организационно - распорядительные документы и внедрять организационные меры по защите информации в автоматизированных системах	ПК-4.1. ***Знать:*** правовые основы организации защиты государственной тайны и/или конфиденциальной информации; задачи органов защиты государственной тайны и/или служб защиты информации на предприятии;	

	отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации Разработка систем защиты информации автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости		свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления; ПК-4.2. ***Знать:*** задачи органов защиты информации на предприятиях; действующие нормативные и методические документы по оформлению рабочей технической документации; понятие и виды террористической деятельности, основы государственной политики Российской Федерации по противодействию терроризму в информационной сфере; нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности значимых объектов критической информационной инфраструктуры; ПК-4.3. ***Знать:*** категории и характеристики	

			значимых объектов критической информационной инфраструктуры; способы выявления угроз информационной безопасности значимых объектов критической информационной инфраструктуры; нормативные документы Российской федерации в области кибербезопасности; особенности организации подразделения центра управления инцидентами (ЦУИ ИБ) для поддержки информационной безопасности промышленной сети; основы правового обеспечения и основные нормативные правовые акты в области защиты информации в различных отраслях деятельности; организацию работы специалистов с документами в автоматизированных системах электронного документооборота	

			ПК-4.4. ***Уметь:*** анализировать правовые акты и осуществлять правовую оценку информации, циркулирующей в автоматизированной системе; квалифицированно исследовать состав документации предприятия (организации);	
			ПК-4.5. ***Уметь:*** разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; реализовывать с учетом особенностей функционирования систем управления значимых объектов критической информационной инфраструктуры требования нормативно-методической и руководящей документации, а также действующего законодательства по вопросам противодействия террористической деятельности	

			ПК-4.6. ***Уметь:*** разрабатывать предложения по совершенствовани ю организационно-распорядительны х документов по безопасности значимых объектов и представлять их руководителю субъекта критической информационной инфраструктуры (уполномоченном у лицу); применять средства юридической защиты информации ограниченного доступа; определять задачи по разработке требований к автоматизированн ым системам обработки и хранения электронных документов	
			ПК-4.7. ***Владеть:*** навыком разработки организационно-распорядительны х документов по защите информации в автоматизированн ых системах; навыком формирования требований по	

			защите информации	
			ПК-4.8. ***Владеть:*** навыком применения современной нормативной базы для построения системы организационных и программно -технических мер по выявлению, предупреждению и пресечению террористической деятельности в отношении систем управления значимых объектов критической информационной инфраструктуры	
			ПК-4.9. ***Владеть:*** навыком использования профессиональной терминологии в области защиты информации в различных отраслях деятельности	
	тип задач профессиональной деятельности - **эксплуатационный**			
	Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической	**ПК-5.** Способен выполнять работы по администрированию систем защиты информации автоматизированных систем и обеспечивать их	ПК-5.1. ***Знать:*** методы и средства контроля и управления доступом при обеспечении безопасности автоматизированных систем; политику	

	информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации Разработка систем защиты информации автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им	работоспособность при возникновении нештатных ситуаций	безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой информационной подсистемы; современные методы предотвращения несанкционированного доступа (НСД) к объектам информатизации, основанные на биометрических технологиях распознавания личности	
			ПК-5.2. ***Знать:*** принципы организации и структуру систем защиты программного обеспечения автоматизированных систем; средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; принципы формирования политики информационной безопасности автоматизированной системы;	

	категорий значимости		основные направления защиты информации в информационно-телекоммуникационных системах в соответствии с законодательством Российской Федерации	
			ПК-5.3. ***Знать:*** современные технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет; архитектуру автоматизированной системы управления технологическим процессом (АСУ ТП), модели промышленных систем автоматизации, сетевые технологии, используемые в современных АСУ ТП, понятия функциональной и информационной безопасности, их взаимосвязь и противоречия; основы организации своевременной и полноценной обработки инцидентов безопасности	
			ПК-5.4. ***Уметь:*** использовать устройства контроля и управления	

			доступом при обеспечении безопасности автоматизированных систем; применять политику безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой информационной подсистемы; использовать устройства контроля доступа на основе биометрических характеристик человека	
			ПК-5.5. ***Уметь:*** регистрировать события, связанные с защитой информации в автоматизированных системах; проводить комплексное тестирование аппаратных и программных средств; определять комплекс мер (правила, процедуры,	

			практические приёмы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; проводить оценку угроз безопасности информационно-телекоммуникационной системы, подключенной к сети Интернет;	
			ПК-5.6. ***Уметь:*** реализовывать технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет; работать со средствами обеспечения безопасности в системах промышленной автоматизации; настраивать межсетевой экран для обеспечения защиты периметра сети, для обеспечения сегментации внутренней сети	
			ПК-5.7. ***Владеть:*** навыком использования систем контроля и управления доступом для управления	

			процессами обеспечения безопасности автоматизированных систем; навыком применения инструментов администрирования подсистем информационной безопасности автоматизированной системы; навыком использования специальных средств биометрической идентификации личности для управления процессами обеспечения безопасности автоматизированных систем	
			ПК-5.8. ***Владеть:*** навыком обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы; навыком обеспечения работоспособности автоматизированных систем при возникновении нештатных ситуаций; навыком разработки частных политик	

			информационной безопасности автоматизированных систем	
			ПК-5.9. ***Владеть:*** навыком использования антивирусного программного обеспечения для защиты информации в информационно-телекоммуникационных системах, подключенных к сети Интернет; анализом инцидентов кибербезопасности в современных промышленных системах автоматизации	
	Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации Разработка систем защиты информации	**ПК-6.** Способен обнаруживать, идентифицировать и устранять инциденты, возникшие в процессе эксплуатации автоматизированных систем	ПК-6.1. ***Знать:*** организационные и технические основы построения систем безопасности значимых объектов критической информационной инфраструктуры и обеспечения их функционирования; угрозы безопасности информации в автоматизированных системах управления и информационных системах;	
			ПК-6.2. ***Знать:*** порядок проведения	

	автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости		расследования компьютерных инцидентов на значимых объектах критической информационной инфраструктуры	
			ПК-6.3. ***Знать:*** меры по восстановлению функционирования и проверке работоспособности значимого объекта критической информационной инфраструктуры в ходе ликвидации последствий компьютерных атак;	
			ПК-6.4. ***Уметь:*** осуществлять реагирование на компьютерные инциденты в порядке, установленном в соответствии с пунктом 6 части 4 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;	
			ПК-6.5. ***Уметь:*** определять источники и причины возникновения компьютерных инцидентов	

			ПК-6.6. ***Уметь:*** определять порядок анализа внештатных ситуаций и принимать меры по недопущению их повторного возникновения;	
			ПК-6.7. ***Владеть:*** навыками обеспечения действий в нештатных ситуациях в ходе эксплуатации значимого объекта критической информационной инфраструктуры;	
			ПК-6.8. ***Владеть:*** реагирования на компьютерные инциденты в ходе эксплуатации значимого объекта критической информационной инфраструктуры;	
			ПК-6.9. ***Владеть:*** навыком проведения расследования инцидентов на средствах вычислительной техники и телекоммуникационном оборудовании значимых объектов критической информационной инфраструктуры	

5. ОБЪЕМ И СТРУКТУРА ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация – **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**)

ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) имеет следующую структуру и состоит из следующих блоков:

Таблица № 3

Структура программы специалитета	Объем программы специалитета и ее блоков в з.е.
Блок 1 «Дисциплины (модули)»	**285**
Обязательная часть	202
Часть, формируемая участниками образовательных отношений	83
Блок 2 «Практики»	**36**
Обязательная часть	12
Часть, формируемая участниками образовательных отношений	24
Блок 3 «Государственная итоговая аттестация»	**9**
Объем программы специалитета	**330**

ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) обеспечивает реализацию дисциплин (модулей) по **философии, истории России, иностранному языку, безопасности жизнедеятельности, основам российской государственности, системам искусственного интеллекта, основам информационной безопасности, организационному и правовому обеспечению информационной безопасности, защите информации от утечки по техническим каналам, методам и средствам криптографической защиты информации, сетям и системам передачи информации, программно-аппаратным средствам защиты информации, управлению информационной безопасностью, разработке и эксплуатации автоматизированных систем в защищенном исполнении** в рамках **Блока 1 «Дисциплины (модули)».**

ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) обеспечивает реализацию дисциплин (модулей) по **физической культуре и спорту**:

в объеме **2 з.е.** в рамках Блока 1 «Дисциплины (модули)»;

в объеме **328 академических часов**, которые являются обязательными для освоения, не переводятся в з.е. и не включаются в объем ОПОП ВО по направлению подготовки **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная), в рамках элективных дисциплин (модулей).

Дисциплины (модули) по **физической культуре и спорту** реализуются в порядке, установленном образовательной организацией. Для инвалидов и лиц с ОВЗ образовательная организация установила особый порядок освоения дисциплин (модулей) по **физической культуре и спорту** с учетом состояния их здоровья.

В **Блок 2 «Практика»** входят **учебные практики,** относящиеся к **обязательной части** программы, и **производственные практики**, относящаяся к **части, формируемой участниками образовательных отношений** (*далее вместе - практики*).

Типы учебной практики:

- ознакомительная практика;
- экспериментально-исследовательская практика.

Типы производственной практики:

- эксплуатационная практика;
- научно-исследовательская работа;
- технологическая практика;
- производственная практика (преддипломная)[1].

Производственная практика (преддипломная) проводится для качественной подготовки и последующего выполнения выпускной квалификационной работы.

[1] установлен дополнительный тип производственной практики, п. 2.6. ФГОС ВО

Практика может проводиться в структурных подразделениях организации. Для лиц с ограниченными возможностями здоровья выбор мест прохождения практик должен учитывать состояние здоровья и требования по доступности.

Практическая подготовка при проведении практики организуется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

Обучающиеся, совмещающие обучение с трудовой деятельностью, вправе проходить практику по месту трудовой деятельности в случаях, если профессиональная деятельность, осуществляемая ими, соответствует требованиям образовательной программы к проведению практики.

Научно-исследовательская работа проводится с целью развития профессиональных компетенций ведения научно-исследовательской деятельности и создания научной основы для написания ВКР. Практика НИР проводится в структурных подразделениях МГРИ.

В **Блок 3 «Государственная итоговая аттестация»** входит **подготовка к процедуре защиты и защита выпускной квалификационной работы.**

Требования к выполнению и защите выпускной квалификационной работы определены локальным нормативным актом образовательной организации, разработанным и утвержденным в соответствии с требованиями приказа Минобрнауки России от 29.06.2015 № 636 (*ред. от 27.03.2020*) «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры» (зарегистрирован Минюстом России 22.07.2015 № 38132).

Защита проводится на заседании государственной экзаменационной комиссии, состав которой утверждается приказом ректора Университета.

Защита ВКР проводится в форме устного доклада, с последующим его обсуждением государственной экзаменационной комиссией. В период действия режима ЧС предусмотрена защита ВКР с применением электронных дистанционных образовательных технологий.

Обучающимся, успешно прошедшим государственную итоговую аттестацию, выдаётся документ об окончании высшего образования и присвоении квалификации «Специалист по защите информации».

Трудоёмкость государственной итоговой аттестации составляет **9 зачётных единиц**.

При разработке ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по**

отрасли или в сфере профессиональной деятельности); форма обучения: очная) обучающимся обеспечивается возможность освоения элективных дисциплин (модулей) и факультативных дисциплин (модулей).

Факультативные дисциплины (модули) не включаются в объем ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности) в области**; форма обучения: очная).

В рамках ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) выделяются **обязательная часть** и **часть, формируемая участниками образовательных отношений**.

К **обязательной части** ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) относятся дисциплины (модули) и практики, обеспечивающие формирование **общепрофессиональных компетенций (ОПК)**, определенных ФГОС ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная).

В обязательную часть ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) включены, в том числе:

дисциплины (модули), указанные в *пункте 5* настоящего документа;

дисциплины (модули) по физической культуре и спорту, реализуемые в рамках Блока 1 «Дисциплины (модули)».

Дисциплины (модули) и практики, обеспечивающие формирование **универсальных компетенций (УК)**, определенных ФГОС ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем**, а также профессиональных компетенций (ПК), определенных образовательной организацией самостоятельно, включены в обязательную часть ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической**

информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности); форма обучения: очная) и в **часть, формируемую участниками образовательных отношений**.

Объем **контактной работы обучающихся с педагогическими работниками Организации при проведении учебных занятий по программе специалитета составляет не менее 50 процентов объема программы специалитета, отводимого на реализацию дисциплин (модулей)** по ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная).

Образовательная организация предоставляет инвалидам и лицам с ОВЗ (*при факте зачисления инвалида и(или) лица с ограниченными возможностями здоровья в образовательную организацию по их заявлению*) возможность обучения по ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная), учитывающей особенности их психофизического развития, индивидуальных возможностей и при необходимости обеспечивающей коррекцию нарушений развития и социальную адаптацию указанных лиц.

6. ПОРЯДОК ОРГАНИЗАЦИИ ПРАКТИЧЕСКОЙ ПОДГОТОВКИ ОБУЧАЮЩИХСЯ,

осваивающих ОПОП ВО по специальности
10.05.03 Информационная безопасность автоматизированных систем
(специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**)

Практическая подготовка обучающегося - форма организации образовательной деятельности при освоении ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) в условиях выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по профилю соответствующей образовательной программы.

Практическая подготовка обучающихся, осваивающих ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная), организуется в соответствии с локальным нормативным актом, разработанным и утвержденным согласно приказу Минобрнауки России № 885, Минпросвещения России № 390 от 05.08.2020 (*ред. от 18.11.2020*) «О практической подготовке обучающихся» (вместе с «Положением о практической подготовке обучающихся») (зарегистрирован Минюстом России 11.09.2020 № 59778).

Практическая подготовка организуется:

- непосредственно в образовательной организации, в том числе в структурном подразделении образовательной организации, предназначенном для проведения практической подготовки;

в организациях, осуществляющих деятельность по профилю ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) (*далее - профильные организации*), в том числе в структурных подразделениях профильных организаций, предназначенных для проведения практической подготовки, на основании договоров, заключенных между образовательной организацией и профильными организациями.

Образовательная деятельность в форме практической подготовки организована при реализации учебных предметов, курсов, дисциплин (модулей), практики, компонентов ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная), предусмотренных учебным планом.

Реализация компонентов ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) в форме практической подготовки может осуществляться непрерывно либо путем чередования с реализацией иных компонентов образовательной программы в соответствии с календарными учебными графиками и учебными планами.

Практическая подготовка при реализации учебных предметов, курсов, дисциплин (модулей) организуется путем проведения практических занятий, практикумов, лабораторных работ и иных аналогичных видов учебной деятельности, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка при проведении практики организуется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

Виды практики и способы ее проведения определены соответствующими рабочими программами, разработанными в соответствии с требованиями ФГОС ВО – специалитет по специальности **10.05.03 Информационная безопасность автоматизированных систем**.

Обучающиеся, совмещающие обучение с трудовой деятельностью, вправе проходить практику по месту трудовой деятельности в случаях, если профессиональная деятельность, осуществляемая ими, соответствует требованиям образовательной программы к проведению практики.

Практическая подготовка включает в себя отдельные занятия лекционного типа, которые предусматривают передачу учебной информации обучающимся, необходимой для последующего выполнения работ, связанных с будущей профессиональной деятельностью.

При организации практической подготовки профильные организации создают условия для реализации компонентов ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной**

инфраструктуры (по отрасли или в сфере профессиональной деятельности); форма обучения: очная), предоставляют оборудование и технические средства обучения в объеме, позволяющем выполнять определенные виды работ, связанные с будущей профессиональной деятельностью обучающихся.

При организации практической подготовки обучающиеся и работники образовательной организации обязаны соблюдать правила внутреннего трудового распорядка профильной организации (образовательной организации, в структурном подразделении которой организуется практическая подготовка), требования охраны труда и техники безопасности.

При наличии в профильной организации или образовательной организации (*при организации практической подготовки в образовательной организации*) вакантной должности, работа на которой соответствует требованиям к практической подготовке, с обучающимся может быть заключен срочный трудовой договор о замещении такой должности.

Практическая подготовка обучающихся с ограниченными возможностями здоровья и инвалидов (*при факте зачисления инвалида и(или) лица с ограниченными возможностями здоровья в образовательную организацию*) организуется с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

Обеспечение обучающихся проездом к месту организации практической подготовки и обратно, а также проживанием их вне места жительства (места пребывания в период освоения ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) в указанный период осуществляется образовательной организацией в порядке, установленном локальным нормативным актом образовательной организации.

7. ТРЕБОВАНИЯ И ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ОПОП ВО

по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация – Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности))

Организация и осуществление образовательной деятельности по ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической**

информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности); форма обучения: очная) регламентированы локальным нормативным актом образовательной организации, разработанным и утвержденным в соответствии с требованиями приказа Минобрнауки России от 06.04.2021 № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры» (зарегистрирован Минюстом России 13.08.2021 № 64644).

7.1. Общесистемные требования к реализации ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**)

Образовательная организация располагает на праве оперативного управления материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) по Блоку 1 «Дисциплины (модули)» и Блоку 3 «Государственная итоговая аттестация» в соответствии с учебным планом.

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

Электронная информационно-образовательная среда образовательной организации обеспечивает:

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

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

В случае реализации ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) с применением электронного обучения, дистанционных образовательных технологий электронная информационно-образовательная среда образовательной организации дополнительно обеспечивает:

- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная);

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

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

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и среды законодательству Российской Федерации.

При реализации ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) в сетевой форме требования к реализации ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) обеспечиваются совокупностью ресурсов материально-технического и учебно-методического обеспечения, предоставляемого организациями, участвующими в реализации программы специалитета в сетевой форме (*при наличии договора о сетевой форме реализации конкретной формы реализации основной образовательной программы высшего образования и соответствующего заявления обучающегося).*

7.2 Требования к материально-техническому и учебно-методическому обеспечению ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**)

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная), оснащенные оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей).

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде образовательной организации.

Допускается замена оборудования его виртуальными аналогами.

Образовательная организация должна быть обеспечена **необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства** (*состав определяется в рабочих программах дисциплин (модулей) и подлежит обновлению при необходимости*).

ЛИЦЕНЗИОННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Office Professional Plus 2019;
2. Project Professional 2016;
3. Windows 10;
4. Webinar Версия 3.0;
5. ПО «Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат. ВУЗ.»;
6. ПО ООО «Лаборатория ММИС»:

Программное обеспечение «Планы»
Программное обеспечение «Деканат»
Программное обеспечение «Приемная комиссия»
Программное обеспечение «Интернет-расширение информационной системы»
Программное обеспечение «Электронные ведомости»
Программное обеспечение «Диплом Мастер»

Программное обеспечение «Визуальная студия тестирования»
Программное обеспечение «Ведомости-Онлайн»
Программное обеспечение «Приемная комиссия-Онлайн»
Программное обеспечение «Тестирование-Онлайн»
Программное обеспечение «Авторасписание AVTOR M» 2 р.м.
Конвертер поручений
Программное обеспечение «Модуль интеграции с суперсервисом «Поступление в вуз онлайн»
Программный модуль для интеграции с ГИС «Современная цифровая образовательная среда».

7. ПО ООО «НПП «ТехАргос»:

- КОМПАС-3D;
- Windows Sandbox;
- MSAT;
- Виртуальные машины сетевого оборудования «RouterOS»;
- Операционная система специального назначения «Astra Linux Special Edition» («Воронеж»);
- Операционная система специального назначения «Astra Linux Common Edition» («Орел»);
- Операционная система общего назначения «Основа»;
- Средство антивирусной защиты информации «Kaspersky Endpoint Security»;
- Средство антивирусной защиты информации «Dr.Web Enterprise Security Suite»;
- Средство антивирусной защиты информации «Avast Antivirus»;
- Средство антивирусной защиты информации «Microsoft Defender»;
- Средства защиты информации «Secret Net Studio 8»;
- Средства защиты информации «Secret Net LSP»;
- Средства защиты информации «Dallas Lock»;
- Программный модуль доверенной загруки «VipNet SafeBoot»;
- Средства защиты информации «vGate R2 Enterprise Plus»;
- Система управления безопасностью корпоративных устройств «Secret MDM»;
- Программа доверенной визуализации и подписи «Jinn-Client-1.x»;
- Высокопроизводительная система обнаружения и предотвращения вторжений с возможностью контроля сетевых приложений «Континент СОВ/СОА»;
- Средство анализа защищенности «Сканер-ВС»;
- Межсетевой экран и система обнаружения вторжений «Рубикон-К»;
- Средство создания модели системы разграничения доступа «Ревизор 1 XP»;
- Программа контроля полномочий доступа к информационным ресурсам «Ревизор 2 XP»;
- Программа фиксации и контроля исходного состояния программного комплекса «Фикс 2.0.2»;

- Программа фиксации и контроля целостности информации «Фикс-Unix 1.0»;
- Программа поиска и гарантированного уничтожения информации на дисках «Terrier 3.0»;
- Средство контроля (анализа) защищенности, тестирования на проникновение «Redcheck PRO»;
- Средство проведения комплексных проверок «Инспектор»;
- Персональный сетевой экран «ViPNet personal Firewall 3.1»;
- Средство криптографической защиты информации «Континент TLS»;
- Аппаратно-программный комплекс шифрования «Континент 3.9»;
- Комплекс безопасности «Континент 4.0»
- Программное средство расчета показателей защищенности информации от утечек по каналам ПЭМИН «Сигурд»;
- SMath Studio;
- LabView;
- SystemView;
- симулятор сети передачи данных «Cisco Packet Tracer»;

СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, в том числе отечественного производства:

- Яндекс браузер;
- Консультант+;
- MISP (Malware Information Sharing Platform)
- WinRar;
- Oracle VM VirtualBox;
- PostgreSQL;
- Hyper-V
- Kali Linux;
- Black Arch
- MS Visual Studio;
- PostgreSQL;
- Blender;
- Djview;
- LyX;
- IPTables;
- Snort;
- Surricata;
- Tcpdump;
- Wireshark;
- Openssl;

- OpenVPN;
- Nmap/zenmap;
- среда программирования Python и R Anaconda;
- nanoCAD;
- САПР Micro-Cap 12;
- Multisim;
- Средство (средства) анализа исходных кодов программ (статический анализатор) Gerrit Code Review;
- Отладчик OnlineGDB
- Компилятор OnlineGDB
- Эмулятор QEMU 3.1.0
- Фаззер MiniFuzz
- Дизассемблер disassembler.io
- Декомпилятор decompiler.com
- Деобфускатор deobfuscate.io
- Распаковщик 7Zzip;
- Шестнадцатеричный редактор HexEd.it
- Средство восстановления формата данных R.saver;
- Средство динамического анализа Iroh.js
- Комплекс для тестирования на проникновение Sparta, Network Infrastructure Penetration Testing Tool.

При использовании в образовательном процессе печатных изданий библиотечный фонд укомплектован печатными изданиями из расчета не менее 0,25 экземпляра каждого из изданий, указанных в рабочих программах дисциплин (модулей), программах 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 определяется в рабочих программах дисциплин (модулей) и подлежит обновлению (*при необходимости*).

СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ:

Электронно-библиотечная система «Лань» (www.e.lanbook.com) (*Доступ к коллекциям "Инженерно-технические науки - Издательство ТИУ (Тюменский индустриальный университет (бывший Тюменский ГНГУ))";*

Электронная библиотечная система «Юрайт» (https://urait.ru/)

Электронная библиотечная система «Библио Тех» (http://www.bibliotech.ru/)

Научная электронная библиотека eLibrary / База данных научных электронных журналов «eLibrary» (http://elibrary.ru)

Издательство с доступом к реферативным и полнотекстовым материалам журналов и книг Wiley (www.wiley.com)

Федеральный портал «Российское образование», Информационная система «Единое окно доступа к образовательным ресурсам» (http://www.edu.ru)

Russian Science Citation Index (RSCI) (https://clarivate.ru)

Международная реферативная база данных «Web of Science Core Collection» (https://apps.webofknowledge.com)

Международная база данных рефератов и цитирования «Scopus» (www.scopus.com)

Полнотекстовая база данных журналов «Nature Journals» (https://nature.com/siteindex)

Информационно-аналитический центр «Минерал» (www.mineral.ru)

Сетевое издание «Нефтегазовое дело» (Open Journal systems) (http://ogbus.ru/)

Золотодобыча. Геология, горное дело, металлургия, обогащение, консалтинг (http://www.zolotodob.ru/)

Аналитическая база данных по странам и отраслям «Полпред» (https://www.polpred.com)

Реферативная база данных по математике «zbMATH» (https://zbmath.org)

База данных в области инжиниринга «Springer Materials» (http://materials.sp.com)

База данных научных протоколов «Springer Nature Experiment» (https://experiments.springernature.com/)

Система «ГАРАНТ» (http://www.garant.ru/)

Система «КонсультантПлюс» (http://www.consultant.ru/)

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья (*при факте зачисления инвалида и(или) лица с ограниченными возможностями здоровья в образовательную организацию*).

7.3 **Требования к кадровым условиям реализации ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**)

Реализация ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) обеспечивается педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) на иных условиях

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

Не менее 70 процентов численности педагогических работников образовательной организации, участвующих в реализации ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная), и лиц, привлекаемых образовательной организацией к реализации ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) на иных условиях (*исходя из количества замещаемых ставок, приведенного к целочисленным значениям*), ведут научную, учебно-методическую и (или) практическую работу, соответствующую профилю преподаваемой дисциплины (модуля).

Не менее 3 процентов численности педагогических работников образовательной организации, участвующих в реализации ОПОП ВО по направлению подготовки **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов**

критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности); форма обучения: очная), и лиц, привлекаемых образовательной организацией к реализации ОПОП ВО по направлению подготовки **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) на иных условиях (*исходя из количества замещаемых ставок, приведенного к целочисленным значениям*), являются руководителями и (или) работниками иных организаций, осуществляющими трудовую деятельность в профессиональной сфере, соответствующей профессиональной деятельности, к которой готовятся выпускники (*имеют стаж работы в данной профессиональной сфере не менее 3 лет*).

Доля педагогических работников Организации (исходя из количества замещаемых ставок, приведенного к целочисленным значениям) должна составлять не менее 65 процентов от общего количества лиц, привлекаемых к реализации программы специалитета.

Не менее 55 процентов численности педагогических работников образовательной организации и лиц, привлекаемых к образовательной деятельности образовательной организации на иных условиях (*исходя из количества замещаемых ставок, приведенного к целочисленным значениям*), имеют ученую степень (*в том числе ученую степень, полученную в иностранном государстве и признаваемую в Российской Федерации*) и (или) ученое звание (*в том числе ученое звание, полученное в иностранном государстве и признаваемое в Российской Федерации*).

В реализации программы специалитета принимает участие один педагогический работник Организации, 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».

В соответствии с профилем ОПОП ВО **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) выпускающей кафедрой является кафедра: Промышленной кибербезопасности и защиты геоданных.

7.4. Требования к финансовым условиям реализации ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем, (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**)

Финансовое обеспечение реализации ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) осуществляется в объёме не ниже установленных Министерством образования и науки Российской Федерации базовых нормативных затрат на оказание государственной услуги в сфере образования для данного уровня образования и направления с учётом корректирующих коэффициентов, учитывающих специфику образовательной программы в соответствии с методикой определения нормативных затрат на оказание государственных услуг по реализации образовательных программ высшего образования по специальностям и направлениям подготовки, утверждённой приказом Министерства образования и науки Российской Федерации от 30 октября 2015 г. № 1272 (зарегистрирован Министерством юстиции Российской Федерации 30 ноября 2015 г., регистрационный № 39898)[2].

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ПРОГРАММАМ СПЕЦИАЛИТЕТА ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ при освоении ими ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем, (специализация – **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**)

Обучение по ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по**

[2] Пункт 10 постановления Правительства Российской Федерации от 26 июня 2015 г. № 640 «О порядке формирования государственного задания на оказание государственных услуг (выполнение работ) в отношении федеральных государственных учреждений и финансового обеспечения выполнения государственного задания» (Собрание законодательства Российской Федерации, 2015, № 28, ст. 4226; 2017, № 38, ст. 5636).

отрасли или в сфере профессиональной деятельности); форма обучения: очная) обучающихся с ограниченными возможностями здоровья осуществляется образовательной организацией с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (*при факте зачисления обучающихся с ограниченными возможностями здоровья в образовательную организацию*).

Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

Образовательной организацией созданы специальные условия для получения высшего образования по ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) обучающимися с ограниченными возможностями здоровья.

Под специальными условиями для получения высшего образования по ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) обучающимися с ограниченными возможностями здоровья понимаются условия обучения, воспитания и развития таких обучающихся, включающие в себя использование специальных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания организаций и другие условия, без которых невозможно или затруднено освоение образовательных программ обучающимися с ограниченными возможностями здоровья.

При получении высшего образования по ОПОП ВО по направлению **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) обучающимся с ограниченными возможностями здоровья предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература, а также услуги сурдопереводчиков и тифлосурдопереводчиков

(*при факте зачисления обучающихся с ограниченными возможностями здоровья в образовательную организацию*).

В целях доступности получения высшего образования по ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) лицами с ограниченными возможностями здоровья организацией обеспечивается (*при факте зачисления обучающихся с ограниченными возможностями здоровья в образовательную организацию*):

а) для лиц с ограниченными возможностями здоровья по зрению:

наличие альтернативной версии официального сайта организации в информационно-телекоммуникационной сети «Интернет» для слабовидящих;

размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме (с учетом их особых потребностей) справочной информации о расписании учебных занятий (информация выполнена крупным рельефно-контрастным шрифтом (на белом или желтом фоне) и продублирована шрифтом Брайля);

присутствие ассистента, оказывающего обучающемуся необходимую помощь (*при факте зачисления обучающихся с ограниченными возможностями здоровья в образовательную организацию*);

обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы) (*при факте зачисления обучающихся с ограниченными возможностями здоровья в образовательную организацию*);

обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию образовательной организации;

б) для лиц с ограниченными возможностями здоровья по слуху:

дублирование звуковой справочной информации о расписании учебных занятий визуальной (установка мониторов с возможностью трансляции субтитров (мониторы, их размеры и количество необходимо определять с учетом размеров помещения));

обеспечение надлежащими звуковыми и визуальными средствами воспроизведения информации;

в) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, материально-технические условия обеспечивают возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, локальное понижение стоек-барьеров, наличие специальных кресел и других приспособлений).

9. ХАРАКТЕРИСТИКА ВОСПИТАТЕЛЬНОЙ СРЕДЫ ВУЗА

Организация воспитательной работы в МГРИ осуществляется на основе взаимодействия имеющихся структур и реализуется на всех уровнях: в образовательном процессе, во внеучебное время, в процессе межличностных контактов.

В университете созданы необходимые условия для формирования компетенций социального взаимодействия, активной жизненной позиции, гражданского самосознания, самоорганизации и самоуправления. В соответствии с этим активно работает студенческое самоуправление, старостаты факультетов, профсоюз студентов и аспирантов, в течение года решающие самостоятельно многие вопросы организации досуга, творческого самовыражения, трудоустройства, межвузовского взаимодействия. Реализуемая в университете модель студенческого самоуправления базируется на предоставлении возможностей каждому обучающемуся самореализоваться, стать участником общественно значимой деятельности, раскрыть свой творческий потенциал в научной, общественно-культурной и спортивной жизни вуза, региона, страны и внести свой посильный вклад в совершенствование системы студенческого самоуправления вуза.

Для организации культурно-творческой, общественно значимой, физкультурно-оздоровительной и спортивной работы на базе МГРИ в настоящее время функционируют 18 студенческих объединений и клубов. Среди них – Студенческий проектный центр, Школа кураторов «Искра», студенческие СМИ, ПУЩ Радио МГРИ, Туристский клуб МГРИ, Школьный факультет, Студенческое объединение «МосДиалог», Волонтерский Центр МГРИ, Совет иностранных обучающихся, Клуб культур, вокально-инструментальная студия, хореографическая студия, кинорежиссерская студия, Студенческий спортивный клуб МГРИ, Киберспортивный клуб МГРИ и др.

Необходимость поддержки инициатив и проектов обучающихся вуза определена как одна из основных задач воспитательной работы университета и заключается в обеспечении социализации и самореализации обучающихся, развитию их потенциала. В рамках содействия развитию студенческих движений и объединений проводятся обучающие семинары, мастер-классы, школы актива и пр., в которых обучающиеся принимают активное участие – как на базе университета, так и на других площадках.

Научно-исследовательская работа обучающихся в вузе рассматривается, как один из важных аспектов повышения качества подготовки и воспитания бакалавров и специалистов.

В вузе активно работают научные кружки и научно-исследовательские группы, такие как MGRI SPE Student Chapter, Студенческое конструкторское бюро, Студенческий проектный центр; организовано участие обучающихся в научных конференция, конкурсах, олимпиадах. Ежегодно на площадке вуза проводится более 50 студенческих научных мероприятий: предметные олимпиады и конкурсы, конференции, семинары международного, всероссийского, регионального и вузовского уровня.

Для организации и проведения выездных воспитательных мероприятий используется Сергиево-Посадский учебно-научно-производственный полигон (Московская обл., Сергиево-Посадский муниципальный р-н), Крымский полигон МГРИ (Республика Крым).

Для организации и проведения физкультурно-спортивных мероприятий используются: спортивный зал МГРИ, залы аэробики, борьбы, бокса, настольного тенниса, бадминтона, тренажерный зал, тир.

Активную научно-образовательную и культурно-просветительскую работу ведут библиотеки и музеи МГРИ – Минералогический музей, Музей занимательной физики, Исторический музей.

Еще одним элементом среды вуза, обеспечивающей решение воспитательных задач, является сайт МГРИ, в котором сосредоточена вся актуальная информация о деятельности вуза, предстоящих мероприятиях.

Портфолио учебных и внеучебных достижений обучающихся позволяет фиксировать развитая информационная электронно-образовательная среда университета.

Рабочая программа воспитания, реализуемая в МГРИ, представлена в Приложении 8.

ОПОП ВО **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) предусматривает проведение различных мероприятий в рамках выполнения общеуниверситетского плана воспитательной работы и с учетом специфики программы подготовки (Приложение 9).

10. ОЦЕНКА КАЧЕСТВА ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ И ПОДГОТОВКИ ОБУЧАЮЩИХСЯ по ОПОП ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем, (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности))

Внешняя оценка качества образовательной деятельности по направлению **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) в рамках процедуры государственной аккредитации проводится с целью подтверждения соответствия требованиям ФГОС ВО: определяется в рамках системы **внутренней оценки**, а также **системы внешней оценки**, в которой Образовательная организация принимает участие на добровольной основе.

В целях совершенствования ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) образовательная организация при проведении регулярной **внутренней оценки качества** образовательной деятельности и подготовки обучающихся по указанной выше программе специалитета привлекает работодателей и (или) их объединения, иных юридических и (или) физических лиц, включая педагогических работников МГРИ.

В рамках **внутренней системы оценки качества** образовательной деятельности по ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) обучающимся систематически предоставляется возможность оценивания условий, содержания, организации и качества образовательного процесса в целом и отдельных дисциплин (модулей) и практик.

Внешняя оценка качества образовательной деятельности по ОПОП ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) в рамках процедуры **государственной аккредитации** осуществлена в 2020 году (приказ Федеральной службы по надзору

в сферу образования и науки от 02.04.2020 № 458, срок действия - бессрочно) с целью подтверждения соответствия образовательной деятельности по указанной выше программе специалитета требованиям ФГОС ВО по специальности **10.05.03 Информационная безопасность автоматизированных систем**.

11. РЕГЛАМЕНТ ПО ОРГАНИЗАЦИИ ПЕРИОДИЧЕСКОГО ОБНОВЛЕНИЯ ОПОП ВО

по специальности **10.05.03 Информационная безопасность автоматизированных систем, (специализация - Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)) в целом, а также составляющих ее компонентов**

Образовательная организация обновляет ОПОП ВО по направлению подготовки **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) (в части перечня дисциплин, установленных МГРИ в учебном плане, и (или) содержания рабочих программ дисциплин (модулей), программ практики и тематики выпускных квалификационных работ, календарного учебного графика, календарного плана воспитательной работы, кадрового состава, материально-технического обеспечения и методических материалов, обеспечивающих реализацию соответствующих образовательных технологий) с учетом развития науки, техники, культуры, экономики, технологий и социальной сферы, запроса со стороны обучающихся и работодателей.

Порядок, форма, условия, технология обновления ОПОП ВО по направлению подготовки **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) установлена локальным нормативным актом образовательной организации.

ОПОП ВО **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) рассмотрена и одобрена на заседании

Ученого Совета Института цифровых технологий недропользования от «20» марта 2025 г., протокол № 25/2.

Председатель Ученого совета Института цифровых технологий недропользования ________________________/ Ладухин О.В./

ОПОП ВО **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) после внесения изменений, рассмотрена и одобрена на заседании Ученого Совета Института цифровых технологий недропользования от «__» _____________ 20___г., протокол №__.

Председатель Ученого совета Института цифровых технологий недропользования ________________________/ Ладухин О.В./

ОПОП ВО **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) после внесения изменений, рассмотрена и одобрена на заседании Ученого Совета Института цифровых технологий недропользования от «__» _____________ 20___г., протокол №__.

Председатель Ученого совета Института цифровых технологий недропользования ________________________/ Ладухин О.В./

ОПОП ВО **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) после внесения изменений, рассмотрена и одобрена на заседании Ученого Совета Института цифровых технологий недропользования от «__» _____________ 20___г., протокол №__.

Председатель Ученого совета Института цифровых технологий недропользования ________________________/ Ладухин О.В./

ОПОП ВО **10.05.03 Информационная безопасность автоматизированных систем** (специализация - **Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)**; форма обучения: очная) после внесения изменений, рассмотрена и одобрена на заседании Ученого Совета Института цифровых технологий недропользования от «__» _____________ 20___г., протокол №__.

Председатель Ученого совета Института цифровых технологий недропользования ________________________/ Ладухин О.В./

Разработчик:
И.о. заведующего кафедрой АРиИ,
к.т.н. _____/Анженко А.А/
(подпись) (ФИО)

Согласовано:
И.о. заведующего кафедрой АРиИ
к.т.н. _____/ Анженко А.А /
(подпись) (ФИО)

Согласовано:
Директор ИЦТН
к.т.н. _____/Ладухин О.В./
(подпись) (ФИО)