Министерство науки и высшего образования Российской Федерации
Федеральное учебно-методическое объединение в системе высшего образования
по УГСН 10.00.00 «Информационная безопасность» (ФУМО ВО ИБ)
Академия ФСБ России
Российский государственный университет нефти и газа (НИУ)
имени И.М. Губкина

Всероссийская научно-практическая конференция

«Кадровое обеспечение субъектов критической информационной инфраструктуры Российской Федерации»

Пленум Федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность»

НАУЧНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Всероссийской научно-практической конференции «Кадровое обеспечение субъектов критической информационной инфраструктуры Российской Федерации» и Пленума ФУМО ВО ИБ

6 – 7 июня 2024 года, г. Москва

Министерство науки и высшего образования Российской Федерации
Федеральное учебно-методическое объединение в системе высшего образования по УГСН 10.00.00 «Информационная безопасность» (ФУМО ВО ИБ)
Академия ФСБ России
Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина

Всероссийская научно-практическая конференция

«Кадровое обеспечение субъектов критической информационной инфраструктуры Российской Федерации»

Пленум Федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность»

НАУЧНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Всероссийской научно-практической конференции «Кадровое обеспечение субъектов критической информационной инфраструктуры Российской Федерации» и Пленума ФУМО ВО ИБ

6 – 7 июня 2024 года, г. Москва

ББК 74.58

НАУЧНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Н 34 **Научно-методические материалы Всероссийской научно-практической конференции «Кадровое обеспечение субъектов критической информационной инфраструктуры Российской Федерации» и Пленума ФУМО ВО ИБ / Москва, 6 – 7 июня 2024: М, 2024 г. – 131 стр.**

Настоящий сборник содержит нормативные материалы в области обеспечения безопасности критической информационной инфраструктуры, научно-методические материалы по проектированию перечня образовательных программ высшего образования в области информационной безопасности в рамках формирования национальной модели высшего образования в Российской Федерации, а также проект ФГОС – 4 по УГСН 34 «Информационная безопасность», подготовленные для обсуждения на Всероссийской научно-практической конференции и Пленуме ФУМО ВО ИБ, проводимого 6 – 7 июня 2024 года.

ФУМО ВО ИБ, оргкомитет Конференции выражают свою признательность всем научно-педагогическим коллективам образовательных организаций и организациям разработчиков средств защиты информации, которые приняли непосредственное участие в организации и проведении Пленума ФУМО ВО ИБ, разработке проекта ФГОС ВО нового поколения в области информационной безопасности.

Особую благодарность выражаем руководству и сотрудникам федерального государственного автономного образовательного учреждения высшего образования «Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина» и лично ректору университета Мартынову В.Г.

Авторский коллектив: Белов Е.Б. (руководитель), Райх В.В., Кабетов Р.В., Шалимов И.А., Киселёв Е.А., Савиных А.Н., Ильков А.В., Хорев А.А., Конев А.А., Правиков Д.И., Лось В.П.

Ответственные за выпуск: Синюков М.Д., Рябков В.Е., Белясова А.Ю.

ББК 74.58

СОДЕРЖАНИЕ

Основные нормативные правовые акты, организационные и методические документы по обеспечению безопасности критической информационной инфраструктуры Российской Федерации

Федеральные законы

Федеральный закон от 26 июля 2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». *Вступил в силу 1 января 2018.*

Федеральный закон от 26 июля 2017 № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»:

- Закон Российской Федерации от 21 июля 1993 № 5485-I «О государственной тайне» (пункт 4 статьи 5);
- Федеральный закон от 7 июля 2003 № 126-ФЗ «О связи» (пункт 11 статьи 12, пункт 1 статьи 46);
- Федеральный закон от 26 декабря 2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (часть 31 статьи 1). *Вступил в силу 1 января 2018.*

Федеральный закон от 26 июля 2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»: уголовный кодекс Российской Федерации (статья 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации)», уголовно- процессуальный кодекс Российской Федерации (статья 151). *Вступил в силу 1 января 2018.*

Федеральный закон от 26 мая 2021 № 141-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»:

- Статья 13.12.1. Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
- Статья 19.7.15. Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
- Статья 23.90. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
- Статья 23.91. Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Вступил в силу по истечении десяти дней после официальной публикации 6 июня 2021, за исключением абзацев третьего и четвёртого пункта 2 статьи 1 настоящего Федерального закона. Абзацы третий и четвёртый пункта 2 статьи 1 настоящего Федерального закона вступили в силу с 1 сентября 2021 (часть 1 статьи 13.12.1).

Федеральный закон от 19 декабря 2022 № 518-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». Изменения в статью 19.7.15. «Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации».

Федеральный закон от 10 июля 2023 № 312-ФЗ «О внесении изменения в статью 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (к субъектам КИИ будут относиться владельцы ИС / ИТС / АСУ из сферы государственной регистрации прав на недвижимое имущество и сделок с ним).

Указы Президента Российской Федерации

Указ Президента РФ от 15 января 2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». *Опубликован и вступил в силу 15 января 2013.*

Указ Президента РФ от 12 декабря 2014 № К 1274 «О Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. *Опубликован 12 декабря 2014.*

Указ Президента РФ от 25 ноября 2017 № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 № 1085». *Опубликован 25 ноября 2017.*

Указ Президента РФ от 8 ноября 2023 № 846 «О внесении изменений в Указ Президента Российской Федерации от 16 августа 2004 № 1085 «Вопросы ФСТЭК России» и в Положение, утверждённое этим Указом».

Указ Президента РФ от 22 декабря 2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». *Опубликован 22 декабря 2017.*

Указ Президента РФ от 2 марта 2018 № 98 «О внесении изменения в перечень сведений, отнесённых к государственной тайне, утверждённый Указом Президента Российской Федерации от 30 ноября 1995 № 1203». *Опубликован 2 марта 2018.*

Указ Президента РФ от 14 апреля 2022 № 203 «О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации». *Опубликован 14 апреля 2022.*

Указ Президента РФ от 30 марта 2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». *Опубликован 30 марта 2022*.

Указ Президента РФ от 1 мая 2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». *Опубликован 1 мая 2022*.

Указ Президента РФ от 26 декабря 2022 № 954 «О внесении изменения в состав Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации по должностям, утверждённый Указом Президента Российской Федерации от 14 апреля 2022 № 203».

Постановления Правительства Российской Федерации

Постановление Правительства РФ от 13 апреля 2019 № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 № 127». *Опубликовано 16 апреля 2019.*

Постановление Правительства РФ от 17 февраля 2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». *Опубликовано 21 февраля 2018.*

Постановление Правительства РФ от 8 февраля 2018 № 127 (ред. от 13 апреля 2019) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». *Опубликовано 16 апреля 2019.*

Постановление Правительства РФ от 8 июня 2019 № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры». *Опубликовано 11 июня 2019.*

Постановление Правительства РФ от 11 июля 2018 № 808 «О внесении изменения в Правила организации повышения квалификации специалистов по ЗИ и должностных лиц, ответственных за организацию ЗИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК». *Опубликовано 13 июля 2018.*

Постановление Правительства РФ от 7 октября 2019 № 1285 «Об утверждении Правил предоставления субсидий из федерального бюджета на создание отраслевого центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и включение его в систему автоматизированного обмена информацией об актуальных киберугрозах». *Опубликовано 9 октября 2019.*

Постановление Правительства РФ от 24 июня 2021 № 981 «Об утверждении Правил формирования и утверждения перечня критически важных объектов». *Опубликовано 28 июня 2021.*

Постановление Правительства РФ от 23 октября 2021 № 1815 «Об утверждении перечня случаев осуществления сбора и обработки используемых для идентификации либо идентификации и аутентификации биометрических персональных данных в информационных системах организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, ……». *Опубликовано 26 октября 2021.*

Постановление Правительства РФ от 24 декабря 2021 № 2431 «О внесении изменений в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации». *Опубликовано 27 декабря 2021.*

Постановление Правительства РФ от 19 августа 2022 № 1463 «О внесении изменения в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации». *Опубликовано 23 августа 2022.*

Постановление Правительства РФ от 22 августа 2022 № 1478 «Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц». на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации». *Опубликовано 26 августа 2022.*

Распоряжение Правительства РФ от 22 июня 2022 № 1661-р (во исполнение Указа № 250) «Об утверждении ключевых органов (организаций), которым необходимо осуществить мероприятия по оценке уровня защищённости своих информационных систем с привлечением организаций, имеющих соответствующие лицензии ФСБ России и ФСТЭК России». *Опубликовано 24 июня 2022.*

Постановление Правительства РФ от 15 июля 2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)». *Опубликовано 19 июля 2022.*

Постановление Правительства РФ от 20 декабря 2022 № 2360 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 № 127». *Опубликовано 21 декабря 2022.*

Постановление Правительства РФ от 17 октября 2023 № 1716 «О внесении изменений в постановление Правительства Российской Федерации от 22 августа 2022 № 1478». *Опубликовано 18 октября 2023.*

Приказы и сообщения Федеральной службы по техническому и экспортному контролю

Приказ ФСТЭК России от 6 декабря 2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрировано в Минюсте России 8 февраля 2018 № 49966).

Опубликован 9 февраля 2018.

Приказ ФСТЭК России от 11 декабря 2017 № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрировано в Минюсте России 28 декабря 2017 № 49500). *Опубликован 28 декабря 2017.*

Приказ ФСТЭК России от 21 декабря 2017 № 235 (ред. от 27 марта 2019) «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (зарегистрировано в Минюсте России 22 февраля 2018 № 50118). Опубликован 14 июня 2019. *Редакция действует с 1 января 2021.*

Информационное сообщение ФСТЭК России от 4 мая 2018 № 240/22/2339 «О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации». *Опубликовано 4 мая 2018.*

Приказ ФСТЭК России от 27 марта 2019 № 64 «О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утверждённые приказом ФСТЭК России от 21 декабря 2017 № 235» (зарегистрировано в Минюсте России 13 июня 2019 № 54920). *Опубликован 14 июня 2019.*

Приказ ФСТЭК России от 22 декабря 2017 № 236 (ред. от 21 марта 2019) «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» (зарегистрировано в Минюсте России 13 апреля 2018 № 50753). *Опубликован 19 апреля 2019.*

Приказ ФСТЭК России от 21 марта 2019 № 59 «О внесении изменений в форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утверждённую приказом ФСТЭК России от 22 декабря 2017 № 236» (зарегистрировано в Минюсте России 18 апреля 2019 № 54436). *Опубликован 19 апреля 2019.*

Приказ ФСТЭК России от 25 декабря 2017 № 239 (в ред. 9 августа 2018 № 138, от 26 марта 2019 № 60, от 20 февраля 2020 № 35) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрировано в Минюсте России 26 марта 2018 № 50524). *Опубликован 14 сентября 2020*.

Приказ ФСТЭК России от 20 февраля 2020 № 35 «О внесении изменений в требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённые приказом ФСТЭК России от 25 декабря 2017 № 239 (зарегистрировано в Минюсте России 11 сентября 2020 № 59793). *Опубликован 14 сентября 2020, вступил в силу 25 сентября 2020, пп.7, 8 изменений вступают в силу 1 января 2023.*

Приказ ФСТЭК России от 26 марта 2019 № 60 «О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённые приказом ФСТЭК России от 25 декабря 2017 № 239» (зарегистрировано в Минюсте России 18 апреля 2019 № 54443). *Опубликован 19 апреля 2019.*

Приказ ФСТЭК России от 28 мая 2020 № 75 «Об утверждении порядка согласования субъектом критической информационной инфраструктуры российской федерации с Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования» (зарегистрировано в Минюсте России 15 сентября 2020 № 59866). *Опубликован 28 мая 2020.*

Приказ ФСТЭК России от 26 апреля 2018 № 72 «О внесении изменений в Регламент ФСТЭК России, утверждённый приказом ФСТЭК России от 12 мая 2005 № 167» (зарегистрировано в Минюсте РФ 18 мая 2018 № 51127). В том числе:

– Абзац второй пункта 9 изложить в следующей редакции: «Обеспечения безопасности значимых объектов критической информационной инфраструктуры»;

– В абзаце третьем пункта 15 слова «информации в ключевых системах» заменить словом «критической». *Вступил в силу 1 июня 2018.*

Приказ ФСТЭК России № 76 от 2 июня 2020 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (зарегистрирован Минюстом России 11 сентября 2020). Отменил приказ ФСТЭК России № 131 от 30 июля 2018 «Об утверждении Требований

по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», дата отмены – с 1 января 2021.

Информационное сообщение ФСТЭК России от 15 октября 2020 № 240/24/4268 «Об утверждении требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий».

Выписка из Требований по безопасности информации, утверждённых приказом ФСТЭК России от 2 июня 2020 № 76.

Методический документ «Методика оценки угроз безопасности информации». *Утверждён ФСТЭК России 5 февраля 2021. Опубликован 5 февраля 2021.*

Приказ ФСТЭК России от 14 марта 2014 № 31 (в ред. от 23 марта 2017 № 49, от 9 августа 2018 № 138, от 15 марта 2021 № 46) «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (зарегистрировано в Минюсте России 30 июня 2014 № 32919).

Информационное сообщение ФСТЭК России от 17 апреля 2020 № 240/84/611 «По вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

Приказ ФСТЭК России от 23 марта 2017 № 49 «О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённые приказом ФСТЭК России от 18 февраля 2013 № 21, и в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утверждённые приказом ФСТЭК России от 14 марта 2014 № 31» (зарегистрировано в Минюсте России 25 апреля 2017 № 46487).

Приказ ФСТЭК России от 9 августа 2018 № 138 «О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утверждённые приказом ФСТЭК России от 14 марта 2014 № 31, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённые приказом ФСТЭК России от 25 декабря 2017 № 239» (зарегистрировано в Минюсте России 5 сентября 2018 № 52071). *Опубликован 6 сентября 2018.*

Приказ ФСТЭК России от 15 марта 2021 № 46 «О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утверждённые приказом ФСТЭК России от 14 марта 2014 № 31» (*зарегистрирован 1 июля 2021 № 64063*).

Письмо ФСТЭК России от 20 марта 2020 № 240/84/389 «Рекомендации по обеспечению безопасности объектов критической информационной инфраструктуры при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов критической информационной инфраструктуры».

Информационное сообщение ФСТЭК России от 18 июня 2021 № 240/82/1037 «О порядке представления субъектами критической информационной инфраструктуры сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий».

Информационное сообщение ФСТЭК России от 18 декабря 2021 № 240/81/2547 «О порядке представления субъектами критической информационной инфраструктуры сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий».

Письмо ФСТЭК России от 28 февраля 2022 № 240/22/952 «О мерах по повышению защищённости информационной инфраструктуры Российской Федерации».

Письмо ФСТЭК России от 6 марта 2022 № 240/22/1172 «О мерах по повышению защищённости информационной инфраструктуры Российской Федерации».

Информационное сообщение ФСТЭК России от 24 марта 2022 № 240/22/1549 «О мерах по повышению защищённости информационной инфраструктуры».

Приказ ФСТЭК России от 10 февраля 2022 № 26 «О внесении изменений в Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённый приказом ФСТЭК России от 6 декабря 2017 № 227».

Информационное сообщение ФСТЭК России от 28 июня 2022 № 240/83/1698. «О порядке представления субъектами критической информационной инфраструктуры сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

Информационное сообщение ФСТЭК России от 28 февраля 2018 № 240/11/879 «О методических рекомендациях по формированию аналитического прогноза по укомплектованию подразделений по обеспечению безопасности значимых объектов критической информационной инфраструктуры, противодействию иностранным техническим разведкам и технической защите информации подготовленными кадрами, утверждённых ФСТЭК России 30 сентября 2016» (в ред. от 9 февраля 2021).

Информационное сообщение ФСТЭК России от 23 апреля 2018 № 240/11/1868 «О методических рекомендациях по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации, разработанных и утверждённых 16 апреля 2018».

Информационное сообщение ФСТЭК России от 28 апреля 2023 № 240/82/818 «О порядке представления субъектами критической информационной инфраструктуры сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

Приказ ФСТЭК России от 20 апреля 2023 № 69 «О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их

функционирования, утверждённые приказом ФСТЭК России от 21 декабря 2017 № 235» (*зарегистрирован 23 июня 2023 № 73969*).

Приказ ФСТЭК России от 1 сентября 2023 № 177 «О внесении изменений в Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённый приказом ФСТЭК России от 6 декабря 2017 № 227» (*зарегистрирован 3 октября 2023 № 75437*).

Приказы и рекомендации Федеральной службы безопасности Российской Федерации

Приказ ФСБ РФ от 24 июля 2018 № 366 «О Национальном координационном центре по компьютерным инцидентам» (зарегистрирован в Минюсте России 6 сентября 2018 № 52109). *Опубликован 10 сентября 2018*.

Приказ ФСБ РФ от 24 июля 2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (зарегистрирован в Минюсте России 6 сентября 2018 № 52108). *Опубликован 10 сентября 2018.*

Приказ ФСБ РФ от 24 июля 2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» (регистрация в Минюсте России 6 сентября 2018 № 52107). *Опубликован 10 сентября 2018.*

Приказ ФСБ РФ от 6 мая 2019 № 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» (зарегистрирован в Минюсте России 31 мая 2019 № 54801). *Опубликован 31 мая 2019.*

Приказ ФСБ РФ от 19 июня 2019 № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» (зарегистрирован в Минюсте России 16 июля 2019 № 55285). *Опубликован 17 июля 2019.*

Приказ ФСБ РФ от 19 июня 2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведённых в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрирован в Минюсте России 16 июля 2019 № 55284). *Опубликован 17 июля 2019.*

Приказ ФСБ РФ от 7 июля 2022 № 348 «О внесении изменений в Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них,

принятия мер по ликвидации последствий компьютерных атак, проведённых в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённый приказом ФСБ России от 19 июня 2019 № 282» (зарегистрирован 5 августа 2022 № 69513).

Приказ ФС РФ от 4 ноября 2022 № 547 «Об утверждении Перечня сведений в области военной, военно-технической деятельности Российской Федерации, которые при их получении иностранными источниками могут быть использованы против безопасности Российской Федерации» (зарегистрирован 17 ноября 2022 № 70986).

Приказ ФСБ РФ от 11 мая 2023 № 213 «Об утверждении порядка осуществления мониторинга защищённости информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими» (зарегистрирован 2 июня 2023 № 73701).

Приказы Минцифры России

Приказ Минцифры РФ от 17 марта 2020 № 114 «Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» (зарегистрирован в Минюсте России 25 июня 2020 № 58753). *Опубликован 25 июня 2020.*

Приказ Минцифры РФ от 28 декабря 2020 № 777 «Об утверждении Рекомендаций по проведению сертификации оборудования связи, используемого в составе сети связи общего пользования, обеспечивающей функционирование значимых объектов критической информационной инфраструктуры».

Приказ Минцифры РФ от 28 декабря 2020 № 779 «Об утверждении организационно-технических мер по обеспечению информационной безопасности ресурсов сети связи общего пользования, используемых значимыми объектами критической информационной инфраструктуры».

Приказ Минцифры РФ № 21 «Об утверждении Методических рекомендаций по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в Российской Федерации».

Отраслевые документы

Минтранс РФ. «Перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере транспорта» *от 19 марта 2023.*

Минэнерго РФ. «Перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере энергетики» *от 8 августа 2023.*

Приказ Министерства промышленности и торговли РФ от 31 мая 2023 № 1981 «Об утверждении Порядка проведения в отношении субъектов критической

информационной инфраструктуры Российской Федерации, осуществляющих деятельность в области оборонной, металлургической и химической промышленности, оценки актуальности и достоверности сведений, указанных в пункте 17 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утверждённых постановлением Правительства Российской Федерации от 8 февраля 2018 № 127, и установлении критериев определения организаций, привлекаемых к оценке актуальности и достоверности сведений, указанных в пункте 17 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утверждённых постановлением Правительства Российской Федерации от 8 февраля 2018 № 127» (зарегистрирован 21 августа 2023 № 74904).

Методические рекомендации по выполнению кредитными и некредитными финансовыми организациями мероприятий по обеспечению безопасности критической информационной инфраструктуры Российской Федерации в части информирования федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о компьютерных инцидентах, результатах мероприятий по реагированию на них и принятии мер по ликвидации последствий компьютерных атак (утверждены Банком России 26 октября 2023 № 15-МР).

Рекомендации
(согласованы со ФСТЭК и ФСБ России)

Методические рекомендации от 26 июня 2019 по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи. Введены в действие для опытного использования в тестовом режиме решением исполкома общественно-государственного объединения «Ассоциация документальной электросвязи». Согласованы: 8 Центр ФСБ России (исх. № 149/2/7-370 от 5 апреля 2019), Общественно-государственное объединение «Ассоциация документальной электросвязи» (протокол от 27 марта 2019), ФСТЭК России (исх. № 240/25/1221 от 18 марта 2019).

Методические рекомендации Минэнерго России по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса. *Опубликованы 1 сентября 2019*. *Согласованы Минэнерго и ФСТЭК России.*

8 Центр ФСБ России. №149/2/7-200 от 24 декабря 2016 «Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

8 Центр ФСБ России. «Временный порядок включения корпоративных центров в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Материалы по актуализации паспорта научной специальности *2.3.6. «Методы и системы защиты информации, информационная безопасность»*

В соответствии с решением Всероссийского форума «Актуальные вопросы подготовки кадров в области информационной безопасности» и совещания ФУМО ВО ИБ от 23 ноября 2023 года в период с 1 февраля по 19 мая 2024 года была проведена работа по актуализации Паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

Экспертами ФУМО ВО ИБ профессорами Шелупановым А.А., Лосем В.П., Хоревым А.А. и профессором РАН Зегждой Д.П. подготовлен актуализированный проект Паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» с учетом замечаний и предложений вузов, поступивших в процессе его обсуждения.

Паспорт научной специальности
2.3.6. «Методы и системы защиты информации, информационная безопасность»

(действующая редакция)

Область науки:

2. Технические науки

Группа научных специальностей:

2.3. Информационные технологии и телекоммуникации

Наименование отрасли науки, по которой присуждаются ученые степени:

Технические

Физико-математические

Шифр научной специальности:

2.3.6. Методы и системы защиты информации, информационная безопасность

Направления исследований:

1. Теория и методология обеспечения информационной безопасности и защиты информации.

2. Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.

3. Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.

4. Системы документооборота (вне зависимости от степени их компьютеризации) и средства зашиты циркулирующей в них информации.

5. Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.

6. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.

7. Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования.

8. Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения.

9. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.

10. Модели и методы оценки защищенности информации и информационной безопасности объекта.

11. Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.

12. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.

13. Методы и модели выявления и противодействия распространению ложной и вредоносной информации.

14. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.

15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

16. Модели, методы и средства обеспечения аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и расследования инцидентов информационной безопасности в автоматизированных информационных системах.

17. Методы, модели и средства разработки безопасного программного обеспечения, выявления в нем дефектов безопасности, противодействия скрытым каналам передачи данных и выявления уязвимостей в компьютерных системах и сетях.

18. Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании.

19. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

Смежные специальности (в т.ч. в рамках группы научной специальности):

1.2.4. Кибербезопасность

2.3.1. Системный анализ, управление и обработка информации

2.3.4. Управление в организационных системах

2.3.8. Информатика и информационные процессы

Паспорт научной специальности
2.3.6. «Методы и системы защиты информации, информационная безопасность»
(предлагаемая актуализированная редакция Паспорта)

Область науки:
2. Технические науки
Группа научных специальностей:
2.3. Информационные технологии и телекоммуникации
Наименование отрасли науки, по которой присуждаются ученые степени:
Технические
Физико-математические
Шифр научной специальности:
2.3.6. Методы и системы защиты информации, информационная безопасность

Направления исследований:

1. Теория и методология защиты информации и обеспечения информационной безопасности.

2. Модели, методы и средства выявления уязвимостей программного обеспечения, протоколов взаимодействия, информационных процессов и систем.

3. Модели, методы, системы и средства выявления угроз безопасности информации на объектах информатизации, в автоматизированных, информационных, киберфизических, самоорганизующихся и телекоммуникационных системах различного назначения, включая компьютерные сети.

4. Модели, методы, системы и средства управления доступом (идентификация, аутентификация, разграничение и контроль доступа).

5. Модели, методы, системы и средства обеспечения и контроля целостности информации, информационных потоков и процессов обработки информации.

6. Модели, методы, системы и средства обнаружения вредоносного программного обеспечения.

7. Модели, методы, системы и средства обеспечения доверия в отношении информационной среды, процессов и технологий.

8. Модели, методы, системы и средства обеспечения надежности, функциональной и киберустойчивости автоматизированных, информационных, киберфизических, самоорганизующихся и телекоммуникационных систем различного назначения, включая компьютерные сети, а так же систем защиты информации.

9. Модели, методы (способы), системы и средства защиты информации от утечки по техническим каналам.

10. Модели, системы и средства защиты информации с использованием криптографических, стеганографических и других методов преобразования информации.

11. Системы и средства (программные, технические, программно-технические), для обеспечения безопасности информации на объектах информатизации, в автоматизированных, информационных, киберфизических, самоорганизующихся и телекоммуникационных системах различного назначения, включая компьютерные сети.

12. Модели, методы, технологии и системы создания безопасного программного обеспечения.

13. Модели, методы, системы и средства обеспечения информационной безопасности систем искусственного интеллекта и машинного обучения.

14. Модели, методы системы, средства обнаружения, предупреждения и противодействия компьютерным атакам и ликвидации их последствий.

15. Модели, методы системы и средства анализа, оценки и управления рисками информационной безопасности.

16. Модели, методы системы, средства аудита, контроля и мониторинга информационной безопасности, а также оценки защищенности автоматизированных, информационных, киберфизических, самоорганизующихся и телекоммуникационных системах различного назначения, включая компьютерные сети

17. Модели, методы системы и средства расследования инцидентов информационной безопасности и компьютерной криминалистики.

18. Модели, методы, методики, системы и средства оценки эффективности защиты информации.

19. Модели, методы и средства оценки соответствия систем и средств защиты информации, программного обеспечения и процессов разработки программного обеспечения по требованиям безопасности информации.

20. Модели, методы, методики и средства проведения специальных исследований и специальных проверок технических средств, проведения специальных обследований выделенных помещений.

21.Модели, методы, системы и средства управления (менеджмента) информационной безопасностью в организациях, в том числе в субъектах критической информационной инфраструктуры.

22. Модели, методы, технологии, системы и средства обеспечения защищенного документооборота.

23. Модели, методы, технологии, системы и средства обеспечения информационной безопасности в социотехнических системах, сети Интернет и в медиапространстве.

Смежные специальности (в т.ч. в рамках группы научной специальности):

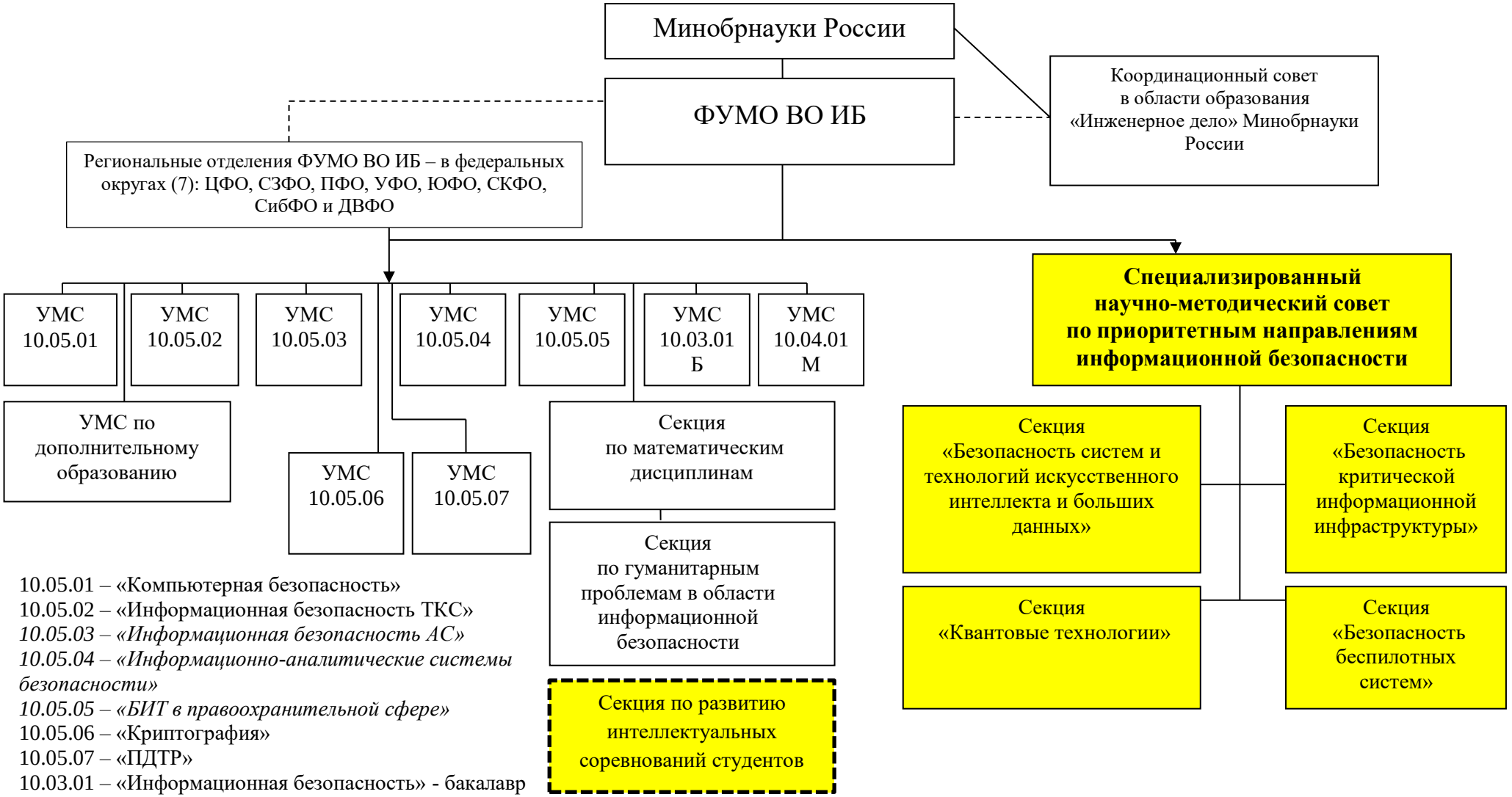
1.2.4. Кибербезопасность

2.3.1. Системный анализ, управление и обработка информации

2.3.4. Управление в организационных системах

2.3.8. Информатика и информационные процессы

Структурная схема
Федерального учебно-методического
объединения в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность»
(ФУМО ВО ИБ)



10.05.01 – «Компьютерная безопасность»
10.05.02 – «Информационная безопасность ТКС»
10.05.03 – «Информационная безопасность АС»
10.05.04 – «Информационно-аналитические системы безопасности»
10.05.05 – «БИТ в правоохранительной сфере»
10.05.06 – «Криптография»
10.05.07 – «ПДТР»
10.03.01 – «Информационная безопасность» - бакалавр
10.04.01 – «Информационная безопасность» - магистр

Нормативная правовая база по регулированию приоритетных направлений ИБ

Секция «Безопасность систем и технологий ИИ и больших данных»	Секция «Безопасность КИИ»	Секция «Квантовые технологии»	Секция «Безопасность беспилотных систем»
1. Национальная стратегия развития ИИ на период до 2030 г. (Указ Президента Российской Федерации от 10.10.2019 № 490). 2. Концепция развития регулирования отношений в сфере технологий ИИ и робототехники до 2024 (Распоряжение Правительства РФ от 19.08.2022 № 2129-р). 3. Поручение ФУМО ВО ИБ от СБ РФ и Минобрнауки России (Решение секции ИБ научного совета при Совете Безопасности РФ протокол № 4 от 12.12.2023 «Об организационных и научных подходах к обеспечению ИБ при использовании технологий ИИ»). 4. Документы технического комитета № 164 «Искусственный интеллект», ТК № 194 «Киберфизические системы», ТК № 26 «Криптографическая защита информации»	1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ». 2. Указ Президента Российской Федерации от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». 3. Указ Президента Российской Федерации от 22.12.2017 № 620 «О совершенствовании ГосСопка на информационные ресурсы РФ». 4. Приказы ФСТЭК России по реализации Федерального закона № 187-ФЗ. 5. Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам». 6. Документы технического комитета № 362 «Защита информации»	1. Распоряжение Правительства РФ от 11.07.2023 № 1856-р «Об утверждении Концепции регулирования отрасли квантовых коммуникаций в РФ до 2030 г.». 2. Поручение ФУМО ВО ИБ от СБ РФ и Минобрнауки Росси (Решение секции ИБ научного совета при Совете Безопасности РФ протокол от 6.10.2023 № 3 «О научных подходах к обеспечению ИБ с использованием квантовых технологий». 3. Письмо от ОАО «РЖД» о вхождении сотрудников ФУМО ВО ИБ в межведомственную рабочую группу «Квантовые коммуникации» от 17.02.2021 № Исх-3335. 4. Дорожные карты «Квантовые вычисления», «Квантовые коммуникации» утв. Правительственной комиссией (протоколы № 14 от 31.07.2020, № 2 от 28.01.2020) 5. Документы ТК № 194 «Киберфизические системы», ТК № 26 «Криптографическая защита информации».	1. Распоряжение Правительства РФ от 21.06.2023 № 1630-р «Об утверждении Стратегии развития беспилотной авиации РФ на период до 2030 г. и на перспективу до 2035 г. и плана мероприятий по ее реализации». 2. Федеральный закон от 04.08.2023 № 440-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». 3. Федеральный закон от 04.08.2023 № 487-ФЗ «О внесении изменений в Воздушный кодекс Российской Федерации».

ПЕРЕЧЕНЬ **ПРОЕКТ**

специальностей и направлений подготовки высшего образования по программам высшего образования и специализированного высшего образования

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОМПЬЮТЕРНЫЕ НАУКИ

Коды УГСН	Коды направлений	Наименования областей образования, УГСН. Наименование специальностей и направлений	Уровень образования	Квалификация	Срок обучения по очной форме
34	**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**				
	01	**Кибербезопасность**	высшее образование	Специалист по защите информации	5,5 лет
	02	**Информационная безопасность телекоммуникационных систем**	высшее образование	Специалист по ЗИ	5,5 лет
	03	**Информационная безопасность автоматизированных систем**	высшее образование	Специалист по ЗИ	5,5 лет
	04	**Информационно-аналитические системы безопасности**	высшее образование	Специалист по ЗИ. Аналитик данных	5,5 лет
	05	**Организация и технологии защиты информации**	высшее образование	Специалист по ЗИ	5 лет
	06	**Криптография***	высшее образование	Специалист по ЗИ. Математик	5 лет
	07	**Противодействие техническим разведкам***	высшее образование	Специалист по ЗИ	5,5 лет
	08	**Информационная безопасность**	специализированное высшее образование	Магистр информационной безопасности	2 года
	09	**Управление информационной безопасностью**	специализированное высшее образование	Магистр по управлению ИБ	1 год

*Укрупненные группы специальностей и направлений подготовки ВО, применяемые при реализации образовательных программ, содержащих сведения, составляющие государственную тайну или служебную информацию ограниченного распространения

Перечень специализаций ФГОС ВО – 4 по УГСН 34 «Информационная безопасность» (Проект)

Кибербезопасность	ИБТКС	ИБАС	ИАСБ	ОТЗИ
1. «Анализ безопасности информационных технологий»; 2. «Математические методы и формальные модели кибербезопасности»; 3. «Разработка защищенного программного обеспечения»; 4. «Разработка средств защиты информации и мониторинга безопасности киберсреды»; 5. «Безопасность информационных технологий объектов критической информационной инфраструктуры» (по отраслям); 6. «Компьютерно-техническая экспертиза, расследование инцидентов информационной безопасности»; 7. «Обнаружение и нейтрализация киберугроз, средства мониторинга киберсреды»; 8. «Кибербезопасность роботизированных (беспилотных) систем»; 9. «Безопасность технологий квантовых вычислений»; 10. «Специальные технологии кибербезопасности».	1. «Мониторинг в телекоммуникационных системах»; 2. «Системы представительской связи»; 3. «Сети специальной связи»; 4. «Системы и сети связи специального назначения»; 5. «Системы специальной связи и информации для органов государственной власти»; 6. «Информационная безопасность аэрокосмических ТКС; 7. «Разработка защищенных ТКС»; 8. «Управление безопасностью ТКСиС»; 9. «Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте» (по видам); 10. «Системы цифровой защищенной связи с подвижными объектами»; 11. «Информационная безопасность квантовых коммуникаций»; 12. «Контроль защищенности информации в телекоммуникационных системах».	1. «Безопасность автоматизированных систем в кредитной-финансовой сфере»; 2. «Безопасность автоматизированных систем на транспорте» (по видам); 3. «Безопасность значимых объектов КИИ» (по отрасли или в сфере профессиональной деятельности); 4. «Безопасность открытых информационных систем»; 5. «Контроль защищенности автоматизированных систем»; 6. «Проектирование автоматизированных систем в защищенном исполнении»; 7. «Безопасность автоматизированных систем управления технологическими процессами» (по отрасли или в сфере профессиональной деятельности); 8. «Мониторинг ИБ автоматизированных систем»; 9. «ИБ ЦОД, облачных и распределенных вычислительных сред» 10. «Безопасность киберфизических систем» 11. «Защита информации в автоматизированных информационных системах специального назначения».	1. «Автоматизация информационно-аналитической деятельности»; 2. «Информационная безопасность финансовых и экономических структур»; 3. «Технологии информационно-аналитического мониторинга»; 4. «Безопасность технологий больших данных»; 5. «Информационная безопасность цифровых платформ социальной коммуникации»; 6. «Математические методы компьютерной безопасности информационно-аналитических систем»; 7. «Безопасность систем искусственного интеллекта»; 8. «Конкурентный цифровой мониторинг и прогнозирование»; 9. «Доверенные квантовые вычисления»; 10. «Информационно-аналитические системы специального назначения».	1. «Техническая защита конфиденциальной информации»; 2. «Организация и проведение компьютерных экспертиз»; 3. «Организационно-правовое обеспечение защиты информации в организации»; 4. «Организация защиты информации (по отраслям или в сфере профессиональной деятельности)»; 5. «Технологии информационного противодействия в социотехнических системах; 6. «Технологии защиты информации в правоохранительной сфере»; 7. «Информационно-аналитическое обеспечение правоохранительной деятельности»; 8. «Оперативно-техническое обеспечение раскрытия и расследования преступлений в сфере компьютерной информации».

Профессиональные стандарты в области информационной безопасности

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

*ПС 06.030 «**Специалист по защите информации в телекоммуникационных системах и сетях**» (Приказ Минтруда России от 14 сентября 2022 г. № 536н. Зарегистрирован в Минюсте России 18.10.2022 рег.№ 70596);*

II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности)

Обобщенные трудовые функции		Трудовые функции	
код	наименование	наименование	уровень квалификации
A	Выполнение комплекса мер по обеспечению функционирования СССЭ (за исключением сетей связи специального назначения) и средств их защиты от НД и компьютерных атак	Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД	5
		Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НД, средств для поиска признаков компьютерных атак в сетях электросвязи	5
		Техническое обслуживание СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НД, средств для поиска признаков компьютерных атак в сетях электросвязи	5
B	Обеспечение защиты от НД и компьютерных атак сооружений и СССЭ (за исключением сетей связи специального назначения) в процессе их эксплуатации	Мониторинг функционирования СССЭ, защищенности от НД и компьютерных атак сооружений и СССЭ	6
		Управление функционированием СССЭ, защищенностью от НД и компьютерных атак сооружений и СССЭ	6
		Управление персоналом, обслуживающим сооружения и СССЭ, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от НД, средства для поиска признаков компьютерных атак в сетях электросвязи	6
C	Обеспечение функционирования средств связи сетей связи специального назначения	Установка средств связи сетей связи специального назначения, включая СКЗИ, средства для поиска признаков компьютерных атак в сетях электросвязи	6
		Обеспечение бесперебойной работы средств связи сетей связи специального назначения, включая СКЗИ, средства для поиска признаков компьютерных атак в сетях электросвязи	6
		Ведение специального делопроизводства и технических документов в процессе эксплуатации средств связи сетей связи специального назначения, включая СКЗИ	6
D	Разработка средств защиты СССЭ (за	Анализ угроз информационной безопасности в сетях электросвязи	7

	исключением сетей связи специального назначения) от НД и компьютерных атак	Разработка средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи ЗТКС	7
		Проведение НИОКР в сфере разработки средств и систем защиты СССЭ от НД, создания ЗТКС	7
E	Обеспечение защиты средств связи сетей связи специального назначения от НД	Организация функционирования сетей связи специального назначения и их средств связи	7
		Проведение НИОКР в сфере разработки сетей связи специального назначения и их средств связи, включая СКЗИ	7
		Контроль защищенности от НД и функциональности сетей связи специального назначения	7
F	Управление развитием средств и систем защиты СССЭ от НД	Управление рисками систем защиты сетей электросвязи от НД	7
		Управление отношениями с поставщиками и потребителями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД	7
		Управление отношениями с регуляторами в сфере защиты информации и обеспечения безопасности критической информационной инфраструктуры Российской Федерации	7
G	Экспертиза проектных решений в сфере защиты СССЭ от НД и компьютерных атак	Исследование эффективности способов, средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи	8
		Разработка технологических процессов производства программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи	8

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

ПС 06.031 ***«Специалист по автоматизации информационно-аналитической деятельности»*** (Приказ Минтруда России от 20 июля 2022 г. № 425н. Зарегистрирован в Минюсте России 22.08.2022 рег.№ 69718);

II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности)

Обобщенные трудовые функции		Трудовые функции	
код	наименование	наименование	уровень квалификации
A	Обслуживание ИАС в защищенном исполнении в процессе эксплуатации	Проведение технического обслуживания ИАС	5
		Ведение технической документации, связанной с эксплуатацией ИАС	5
		Обеспечение защиты информации при выводе из эксплуатации ИАС	5
B	Решение задач АИАД с использованием ИАС в защищенном исполнении	Автоматизированная информационно-аналитическая поддержка процессов принятия решений	6
		Решение типичных задач обработки информации в ИАС	6
		Решение типичных задач анализа информации в ИАС	6
		Настройка ИАС для решения задач в сфере профессиональной деятельности	6

		Обеспечение функционирования ИАС	6
		Обеспечение функционирования средств защиты информации в ИАС	6
		Управление работой коллектива информационно-аналитических работников и специалистов по созданию и эксплуатации ИАС	6
		Разработка нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование ИАС	6
		Организация работ по выполнению в ИАС требований защиты информации ограниченного доступа	6
C	Проектирование ИАС в защищенном исполнении	Проведение предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений	7
		Выбор технологии и основных компонентов обеспечивающей части создаваемых ИАС	7
		Разработка проектных документов на создаваемые ИАС	7
		Проектирование обеспечивающей части ИАС	7
		Исследование эффективности ИАС	7
D	Проведение исследований в области эффективных технологий АИАД	Анализ и обобщение результатов научных исследований и разработок в области технологий АИАД	8
		Моделирование и исследование технологий АИАД	8
		Выработка и внедрение научно обоснованных решений, повышающих эффективность технологий АИАД	8

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

*ПС 06.032 «**Специалист по безопасности компьютерных систем и сетей**» (Приказ Минтруда России от 14 сентября 2022 г. № 533н. Зарегистрирован в Минюсте России 14.10.2022 рег.№ 70515);*

II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности)

Обобщенные трудовые функции		Трудовые функции	
код	наименование	наименование	уровень квалификации
A	Техническое обслуживание средств защиты информации в компьютерных системах и сетях	Техническое обслуживание программно аппаратных средств защиты информации в операционных системах	5
		Техническое обслуживание программно аппаратных средств защиты информации в компьютерных сетях	5
		Техническое обслуживание средств защиты информации прикладного и системного программного обеспечения	5
B	Администрирование средств защиты информации в компьютерных системах и сетях	Администрирование подсистем защиты информации в операционных системах	6
		Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	6
		Администрирование средств защиты информации прикладного и системного программного обеспечения	6

C	Оценивание уровня безопасности компьютерных систем и сетей	Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации в компьютерных системах и сетях	7
		Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей	7
		Проведение анализа безопасности компьютерных систем	7
		Проведение сертификации программно-аппаратных средств защиты информации	7
		Проведение инструментального мониторинга защищенности компьютерных систем и сетей	7
		Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях	7
D	Разработка программно-аппаратных средств защиты информации компьютерных систем и сетей	Разработка требований к программно-аппаратным средствам защиты информации компьютерных систем и сетей	8
		Проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей	8
		Разработка и тестирование средств защиты информации компьютерных систем и сетей	8
		Сопровождение разработки средств защиты информации компьютерных систем и сетей	8
A	Техническое обслуживание средств защиты информации в компьютерных системах и сетях	Техническое обслуживание программно-аппаратных средств защиты информации в операционных системах	5
		Техническое обслуживание программно-аппаратных средств защиты информации в компьютерных сетях	5
		Техническое обслуживание средств защиты информации прикладного и системного программного обеспечения	5
E	Руководство разработкой программно-аппаратных средств защиты информации компьютерных систем и сетей	Руководство разработкой требований к программно-аппаратным средствам защиты информации компьютерных систем и сетей	8
		Руководство проектированием программно-аппаратных средств защиты информации компьютерных систем и сетей	8
		Руководство разработкой и тестированием средств защиты информации компьютерных систем и сетей	8
		Руководство сопровождением разработки средств защиты информации компьютерных систем и сетей	8

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

*ПС 06.033 «**Специалист по защите информации в автоматизированных системах**» (Приказ Минтруда России от 14 сентября 2022 г. № 525н. Зарегистрирован в Минюсте России 14.10.2022 рег.№ 70543);*

II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности)

Обобщенные трудовые функции		Трудовые функции	
код	наименование	наименование	уровень квалификации
A	Обслуживание систем защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости	Проведение технического обслуживания систем защиты информации автоматизированных систем	5
		Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем	5
		Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем	5
B	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	Диагностика систем защиты информации автоматизированных систем	6
		Администрирование систем защиты информации автоматизированных систем	6
		Управление защитой информации в автоматизированных системах	6
		Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций	6
		Мониторинг защищенности информации в автоматизированных системах	6
		Аудит защищенности информации в автоматизированных системах	6
		Установка и настройка средств защиты информации в автоматизированных системах	6
		Разработка организационно-распорядительных документов по защите информации в автоматизированных системах	6
		Анализ уязвимостей внедряемой системы защиты информации	6
		Внедрение организационных мер по защите информации в автоматизированных системах	6
C	Разработка систем защиты информации	Тестирование систем защиты информации автоматизированных систем	7

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

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

*ПС 06.034 «**Специалист по технической защите информации**»*
(Приказ Минтруда России от 09 августа 2022 г. № 474н. Зарегистрирован в Минюсте России 09.09.2022 рег.№ 70015).

II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности)

Обобщенные трудовые функции		Трудовые функции	
код	наименование	наименование	уровень квалификации
A	Проведение работ по установке и техническому обслуживанию средств защиты информации	Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты акустической речевой информации от ее утечки по техническим каналам	5
		Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программных (программно-технических) средств защиты информации от несанкционированного доступа	5

B	Проведение работ по установке и техническому обслуживанию защищенных средств обработки информации	Проведение работ по установке, настройке, испытаниям и техническому обслуживанию защищенных технических средств обработки информации	6
C	Производство, сервисное обслуживание и ремонт средств защиты информации от утечки по техническим каналам	Производство, сервисное обслуживание и ремонт технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок	6
		Производство, сервисное обслуживание и ремонт технических средств защиты акустической речевой информации от утечки по техническим каналам	6
		Производство, сервисное обслуживание и ремонт защищенных технических средств обработки информации	6
		Производство, сервисное обслуживание и ремонт технических средств контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок	6
D	Производство, сервисное обслуживание и ремонт средств защиты информации от несанкционированного доступа	Производство, сервисное обслуживание и ремонт программных (программно-технических) средств защиты информации от несанкционированного доступа	6
		Производство, сервисное обслуживание и ремонт программных (программно-технических) средств контроля защищенности информации от несанкционированного доступа	6
E	Проведение контроля защищенности информации	Проведение специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации	6
		Проведение контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	6
		Проведение контроля защищенности акустической речевой информации от утечки по техническим каналам	6
		Проведение контроля защищенности информации от несанкционированного доступа	6
F	Разработка средств защиты информации от утечки по техническим каналам	Разработка технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок	7
		Разработка технических средств защиты акустической речевой информации от утечки по техническим каналам	7
		Разработка защищенных технических средств обработки информации	7
		Разработка технических средств контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок	7
		Разработка технических средств контроля эффективности защиты акустической речевой информации от утечки по техническим каналам	7
G	Разработка средств защиты информации от несанкционированного доступа	Разработка программных (программно-технических) средств защиты информации от несанкционированного доступа	7
		Разработка защищенных программных (программно-технических) средств обработки информации	7

		Разработка программных (программно-технических) средств контроля защищенности информации от несанкционированного доступа	7
H	Проектирование объектов информатизации в защищенном исполнении	Проектирование ОВТ в защищенном исполнении	7
		Проектирование выделенных (защищаемых) помещений	7
I	Проведение аттестации объектов информатизации на соответствие требованиям по защите информации	Проведение аттестации ОВТ на соответствие требованиям по защите информации	7
		Проведение аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации	7
J	Проведение сертификационных испытаний средств защиты информации от утечки по техническим каналам	Проведение сертификационных испытаний технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок	7
		Проведение сертификационных испытаний технических средств защиты акустической речевой информации от утечки по техническим каналам	7
		Проведение сертификационных испытаний защищенных технических средств обработки информации	7
		Проведение сертификационных испытаний технических средств контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок	7
		Проведение сертификационных испытаний технических средств контроля эффективности защиты акустической речевой информации от утечки по техническим каналам	7
		Проведение сертификационных испытаний средств защиты информации от несанкционированного доступа	7
		Проведение сертификационных испытаний программных (программно-технических) средств контроля защищенности информации от несанкционированного доступа	7
		Организация и проведение работ по защите информации в организации	7
		Аналитическое обоснование необходимости создания системы защиты информации в организации	8
		Ввод в эксплуатацию системы защиты информации в организации	7
		Сопровождение системы защиты информации в ходе ее эксплуатации	7

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

ПС 06.053 ***«Специалист по информационной безопасности в кредитно-финансовой сфере»*** *(Приказ Минтруда России от 28 ноября 2022 г. № 739н. Зарегистрирован в Минюсте России 22.12.2022 рег.№ 71784);*

II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности

Обобщенные трудовые функции		Трудовые функции	
код	наименование	наименование	уровень квалификации
A	Обеспечение функционирования систем и средств защиты информации в организациях КФС	Проведение работ по установке, настройке и техническому обслуживанию систем и средств защиты информации в организациях КФС	6
		Администрирование систем и средств защиты информации в организациях КФС	6
		Реализация процессов обеспечения операционной надежности (киберустойчивости) в организациях КФС	6
B	Управление инцидентами информационной безопасности в организациях КФС	Выявление и регистрация инцидентов информационной безопасности, в том числе обнаружение компьютерных атак, в организациях КФС	7
		Реагирование на инциденты информационной безопасности в организациях КФС	7
		Восстановление функционирования бизнес-процессов и технологических процессов и объектов информатизации после реализации инцидентов информационной безопасности в организациях КФС	7
C	Аналитическое и организационное сопровождение деятельности по управлению рисками информационной безопасности в организациях КФС	Сбор и регистрация информации о выявленных рисках информационной безопасности в организациях КФС	7
		Разработка мероприятий, направленных на уменьшение негативного влияния рисков информационной безопасности в организациях КФС	7
		Определение угроз информационной безопасности в организациях КФС	7
		Выявление, идентификация и оценка рисков информационной безопасности в организациях КФС	7
		Мониторинг рисков информационной безопасности и контроль показателей уровня рисков информационной безопасности в организациях КФС	7
		Обеспечение информационной безопасности значимых объектов критической информационной инфраструктуры в организациях КФС	7
		Организация защиты информации, в том числе защиты персональных данных, в организациях КФС	7
		Обеспечение операционной надежности (киберустойчивости) в организациях КФС	7
D	Методологическое обеспечение процессов	Разработка политики в области обеспечения информационной безопасности, по вопросам управления рисками информационной безопасности, обеспечения	7

	информационной безопасности в организациях КФС	операционной надежности (киберустойчивости) и защиты информации в организациях КФС	
		Разработка методологии обеспечения защиты информации и операционной надежности (киберустойчивости) в организациях КФС	7
		Разработка методологии управления рисками информационной безопасности в организациях КФС	7
		Разработка методологии выявления инцидентов информационной безопасности, реагирования на них и восстановления после их реализации в организациях КФС	7
E	Контроль обеспечения информационной безопасности и обеспечение операционной надежности (киберустойчивости) в организациях КФС	Проведение контрольных проверок работоспособности и оценка эффективности применяемых программно-аппаратных средств защиты информации в организациях КФС	7
		Контроль процессов защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС	7
		Реализация программ повышения осведомленности организаций КФС по вопросам защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС	7
F	Организация процессов обеспечения информационной безопасности в организациях КФС	Организация управления рисками информационной безопасности на высшем управленческом уровне в организациях КФС	8
		Организация обеспечения защиты информации и операционной надежности (киберустойчивости) на высшем управленческом уровне в организациях КФС	8
		Контроль процедур управления рисками информационной безопасности и обеспечения защиты информации и операционной надежности (киберустойчивости) на высшем управленческом уровне в организациях КФС	8
		Совершенствование системы управления рисками информационной безопасности, обеспечение защиты информации и операционной надежности (киберустойчивости) на высшем управленческом уровне в организациях КФС	8

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 15 июля 2022 г. № 1272

(ВЫПИСКА)

Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)

В соответствии с подпунктом "а" пункта 3 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" Правительство Российской Федерации постановляет:

Утвердить прилагаемые:

типовое положение о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации);

типовое положение о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации).

ТИПОВОЕ ПОЛОЖЕНИЕ о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации)

II. Квалификационные требования к ответственному лицу

6. Ответственное лицо должно иметь высшее образование (не ниже уровня специалитета, магистратуры) по направлению обеспечения информационной безопасности. Если ответственное лицо имеет высшее образование по другому направлению подготовки (специальности), он должен пройти обучение по программе профессиональной переподготовки по направлению "Информационная безопасность".

7. Для ответственного лица требуются наличие следующих знаний, умений и профессиональных компетенций:

а) основные (в том числе производственные, бизнес и управленческие) процессы органа (организации) и специфика обеспечения информационной безопасности органа (организации);

б) влияние информационных технологий на деятельность органа (организации), в том числе:

роль и место информационных технологий (в том числе степень интеграции информационных технологий) в процессах функционирования органа (организации);

зависимость основных процессов функционирования органа (организации) от информационных технологий;

в) информационно-телекоммуникационные технологии, в том числе:

современные информационно-телекоммуникационные технологии, используемые в органе (организации);

способы построения информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления формирования информационных ресурсов (далее - системы и сети), в том числе ограниченного доступа;

типовые архитектуры систем и сетей, требования к их оснащенности программными (программно-техническими) средствами;

принципы построения и функционирования современных операционных систем, систем управления базами данных, систем и сетей, основных протоколов систем и сетей;

г) обеспечение информационной безопасности, в том числе: цели, задачи, основы организации, ключевые элементы, основные способы и средства обеспечения информационной безопасности;

цели обеспечения информационной безопасности применительно к основным процессам функционирования органа (организации), реализации и контроля их достижения;

принципы и направления стратегического развития информационной безопасности в органе (организации);

правила разработки, утверждения и отмены организационно-распорядительных документов по вопросам обеспечения информационной безопасности в органе (организации), состав и содержание таких документов;

порядок организации работ по обеспечению информационной безопасности в органе (организации);

основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации, способы и методы обеспечения и поддержания необходимого уровня (состояния) информационной безопасности органа (организации) для исключения (невозможности реализации) негативных последствий, а также порядок проведения практических проверок и контроля результативности применяемых способов и методов обеспечения информационной безопасности органа (организации);

основные угрозы безопасности информации, предпосылки их возникновения и возможные пути их реализации, а также порядок оценки таких угроз;

возможности и назначения типовых программных, программно-аппаратных (технических) средств обеспечения информационной безопасности;

способы и средства проведения компьютерных атак, актуальные тактики и техники нарушителей;

порядок организации взаимодействия структурных подразделений органа (организации) при решении вопросов обеспечения информационной безопасности;

управление проектами по информационной безопасности;

антикризисное управление и принятие управленческих решений при реагировании на кризисы и компьютерные инциденты;

планирование деятельности по обеспечению информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах);

формулирование измеримых и практических результатов деятельности по обеспечению информационной безопасности органа (организации), подведомственных организаций (филиалов, представительств);

организация разработки политики (правил, процедур), регламентирующей вопросы информационной безопасности в органе (организации), в подведомственных организациях (филиалах, представительствах) (далее - политика);

внедрение политики;

организация контроля и анализа применения политики;

организация мероприятий по разработке единых инструментов и механизмов контроля деятельности по обеспечению информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах);

поддержка и совершенствование деятельности по обеспечению информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах);

организация мероприятий по определению угроз безопасности информации систем и сетей, а также по формированию требований к обеспечению информационной безопасности в органе (организации);

организация внедрения способов и средств для обеспечения информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах);

организация мероприятий по анализу и контролю состояния информационной безопасности органа (организации) и модернизации (трансформации) процессов функционирования органа (организации) в целях обеспечения информационной безопасности в органе (организации)

обеспечение информационной безопасности в ходе эксплуатации систем и сетей, а также при выводе их из эксплуатации;

организация мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы органа (организации) и реагированию на компьютерные инциденты;

организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) в органе (организации), подведомственных организациях (филиалах, представительствах)

8. С учетом области и вида деятельности органа (организации) от ответственного лица требуется знание нормативных правовых актов Российской Федерации, методических документов, международных и национальных стандартов в области:

а) защиты государственной тайны;

б) защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных;

в) обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

г) обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

д) создания и обеспечения безопасного функционирования государственных информационных систем и информационных систем в защищенном исполнении;

е) создания, обеспечения технических условий установки и эксплуатации средств защиты информации;

ж) иных нормативных правовых актов и стандартов в области информационной безопасности.

ПРОЕКТ 28 мая 2024 г.
7 итерация

Федеральный государственный образовательный стандарт высшего образования по укрупненной группе специальностей и направлений подготовки 34 «Информационная безопасность»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий федеральный государственный образовательный стандарт высшего образования (далее – ФГОС ВО) представляет собой совокупность обязательных требований при реализации основных профессиональных образовательных программ высшего образования: программ базового высшего образования – программ специалитета, программ специализированного высшего образования – программ магистратуры по направлениям подготовки, отнесенным к укрупненной группе специальностей и направлений подготовки высшего образования 34 «Информационная безопасность» (далее соответственно – образовательная программа, программа базового высшего образования – программа по специальности, программа специализированного высшего образования – программа по направлению подготовки магистратуры).

1.2. Состав укрупненной группы специальностей и направлений подготовки высшего образования (далее – УГСН) 34 «Информационная безопасность» определяется перечнем специальностей и направлений подготовки высшего образования[1].

1.3. Получение образования по программам базового высшего образования допускается только в образовательной организации высшего образования.

Получение образования по программам специализированного высшего образования допускается только в образовательных организациях высшего образования и научных организациях (далее вместе – Организация).

1.4. К освоению программ специализированного высшего образования за счет средств федерального бюджета, бюджетов субъектов Российской Федерации и местных бюджетов допускаются лица, имеющие диплом по специальностям базового высшего образования, указанным в приложении к настоящему ФГОС ВО.

1.5. Обучение по образовательной программе в Организации может осуществляться в очной и очно-заочной формах, определяемых в соответствии с характеристикой соответствующей программы по специальности,

[1] Часть 8 статьи 11 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (Собрание законодательства Российской Федерации, 2012, № 53, ст. 7598; 2018, № 32, ст. 5110).

по направлению подготовки магистратуры, установленной в разделе 5 настоящего ФГОС ВО (далее – Характеристика образовательной программы).

1.6. Содержание высшего образования по специальностям и направлениям подготовки, отнесенным к УГСН 34 «Информационная безопасность», определяется программой базового высшего образования – программой по специальности, программой специализированного высшего образования – программой по направлению подготовки магистратуры, разрабатываемой и утверждаемой Организацией самостоятельно в соответствии с ФГОС ВО.

При разработке образовательной программы Организация формирует требования к результатам ее освоения в виде универсальных, базовых, общепрофессиональных и профессиональных компетенций выпускников (далее вместе – компетенции) в соответствии с Характеристикой образовательной программы.

1.7. Организация вправе разрабатывать образовательную программу, включающую в себя компетенции, отнесенные к одной или нескольким направлениям по соответствующим уровням профессионального образования или к УГСН, а также к области (областям) и виду (видам) профессиональной деятельности, в том числе с учетом возможности одновременного получения обучающимися нескольких квалификаций[2].

При разработке образовательной программы с учетом возможности одновременного получения обучающимися нескольких квалификаций Организация исходит из квалификаций, указанных в Перечней специальностей и направлений подготовки высшего образования[3], квалификаций квалифицированного рабочего, служащего, указанных в Перечне профессий среднего профессионального образования[4], а также квалификаций, которые формируются по итогам реализации программ дополнительного профессионального образования и квалификаций, которые размещаются в том числе в Реестре сведений о проведении независимой оценки квалификаций[5].

1.8. При реализации образовательной программы Организация вправе применять электронное обучение, дистанционные образовательные технологии.

Реализация всех образовательных программ, отнесенных к УГСН 34 «Информационная безопасность», с применением исключительно электронного

---

[2] Часть 8.1 статьи 12 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (Собрание законодательства Российской Федерации, 2012, № 53, ст. 7598; 2018, № 32, ст. 5110).

[3] Приказ Министерства науки и высшего образования Российской Федерации от 1 февраля 2022 г. № 89 (зарегистрирован Министерством юстиции Российской Федерации 3 марта 2022 г., регистрационный № 67610).

[4] Приказ Министерства образования и науки Российской Федерации от 29 октября 2013 г. № 1199 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2013 г., регистрационный № 30861).

[5] Приказ Министерства труда и социальной защиты Российской Федерации от 15 ноября 2016 г. № 649н «Об утверждении порядка формирования и ведения реестра сведений о проведении независимой оценки квалификации и доступа к ним, а также перечня сведений, содержащихся в указанном реестре» (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2013 г., регистрационный № 30861).

обучения, дистанционных образовательных технологий не допускается[6].

Максимальный объем занятий обучающегося с применением электронного обучения, дистанционных образовательных технологий определяется Характеристикой образовательной программы.

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

1.9. Реализация образовательной программы Организацией допускается с использованием сетевой формы.

1.10. Образовательная программа реализуется на государственном языке Российской Федерации, если иное не определено локальным нормативным актом Организации[7].

1.11. При разработке программы базового высшего образования – программы по специальности Организация выбирает направленность (профиль, специализацию) образовательной программы из перечня, определенного Характеристикой образовательной программы.

При разработке программы специализированного высшего образования – программы по направлению подготовки магистратуры Организация устанавливает направленность (профиль, специализацию) образовательной программы, которая соответствует специальности(ям) или направлению(ям) подготовки высшего образования в целом или конкретизирует содержание образовательной программы в рамках направления(ий) подготовки или специальности(ей) высшего образования путем ориентации ее на область (области) профессиональной деятельности и (или) сферу (сферы) и/или объект (объекты) профессиональной деятельности выпускников и (или) иные требования рынка труда.

1.12. Образовательная программа, содержащая сведения, составляющие государственную и служебную тайну, разрабатывается и реализуется с соблюдением требований, предусмотренных законодательством Российской Федерации и иными нормативными правовыми актами в области защиты государственной и служебной тайны.

1.13. Образовательные программы, отнесенные к УГСН 34 «Информационная безопасность», реализуемые в интересах обороны и безопасности государства, обеспечения законности и правопорядка в федеральных государственных образовательных организациях, находящихся в ведении

[6] Часть 3 статьи 16 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (Собрание законодательства Российской Федерации, 2012, № 53, ст. 7598; 2019, № 30, ст. 4134).

[7] Статья 14 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (Собрание законодательства Российской Федерации, 2012, № 53, ст. 7598; 2018, № 32, ст. 5110).

федеральных государственных органов, указанных в части 1 статьи 81 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (далее – федеральные государственные организации, осуществляющие подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка), разрабатывается на основе требований, предусмотренных указанным Федеральным законом, а также квалификационных требований к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемых федеральным государственным органом, в ведении которого находятся соответствующие организации[8].

2. ТРЕБОВАНИЯ К СТРУКТУРЕ И ОБЪЕМУ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Объем образовательной программы устанавливается в соответствии с Характеристикой образовательной программы.

Объем образовательной программы, разработанной с учетом возможности одновременного получения обучающимися нескольких квалификаций[9], может быть увеличен по решению Организации не более чем на 60 з.е.

Получение квалификации по программам базового высшего образования, программам магистратуры, отнесенных к укрупненной группе 34 «Информационная безопасность», в рамках реализации образовательных программ иных укрупненных групп не допускается.

2.2. Срок получения образования по образовательной программе (вне зависимости от применяемых образовательных технологий) в очной форме обучения устанавливается в соответствии с Характеристикой образовательной программы.

Срок получения образования по программе базового высшего образования в очно-заочной форме обучения увеличивается не менее чем на 6 месяцев и не более чем на 1 год по сравнению со сроком получения образования в очной форме обучения.

Срок получения образования по программе специализированного высшего образования в очно-заочной форме обучения увеличивается не менее чем на 3 месяца и не более чем на 6 месяцев по сравнению со сроком получения образования в очной форме обучения.

[8] Часть 2 статьи 81 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (Собрание законодательства Российской Федерации, 2012, № 53, ст. 7598; 2016, № 27, ст. 4238).

[9] Подпункт 6 части 1 статья 34 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (Собрание законодательства Российской Федерации, 2012, № 53, ст. 7598; 2018, № 32, ст. 5110).

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

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

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, объем образовательной программы, реализуемый за один учебный год по очной форме, составляет не более 75 з.е.

2.4. Организация самостоятельно определяет в пределах сроков и объемов, установленных пунктами 2.1 и 2.2 ФГОС ВО:

срок получения образования по образовательной программе в очно-заочной форме обучения, по индивидуальному учебному плану, в том числе при ускоренном обучении;

срок получения образования по образовательной программе с учетом возможности одновременного получения обучающимися нескольких квалификаций;

объем образовательных программ, реализуемый за один учебный год.

2.5. Структура образовательной программы включает следующие блоки:

Блок 1 «Дисциплины (модули)»;

Блок 2 «Практика»;

Блок 3 «Государственная итоговая аттестация».

2.6. Программа базового высшего образования в рамках Блока 1 «Дисциплины (модули)» должна обеспечивать:

- реализацию дисциплин (модулей) по философии, иностранному языку, безопасности жизнедеятельности, основам информационной безопасности, организационному и правовому обеспечению информационной безопасности, методам и средствам криптографической защиты информации, защите информации от утечки по техническим каналам *(на обсуждение)*;

- реализацию дисциплин (модулей), определенных Характеристикой образовательной программы;

- реализацию дисциплины (модуля) «История России» в объеме не менее 4 з.е., при этом объем занятий в форме контактной работы обучающихся с педагогическими работниками Организации и (или) лицами, привлекаемыми организацией к реализации образовательной программы на иных условиях, должен составлять в очной форме обучения не менее 80 процентов

объема, отводимого на реализацию указанной дисциплины (модуля);

- реализацию дисциплин (модулей) по физической культуре и спорту:

в объеме не менее 2 з.е.;

в объеме не менее 328 академических часов, которые являются обязательными для освоения, не переводятся в з.е. и не включаются в объем программы базового высшего образования, в рамках элективных дисциплин (модулей).

Дисциплины (модули) по физической культуре и спорту реализуются в порядке, установленном Организацией.

Для инвалидов и лиц с ОВЗ Организация устанавливает особый порядок освоения дисциплин (модулей) по физической культуре и спорту с учетом состояния их здоровья.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, вместо дисциплин (модулей) по физической культуре и спорту в рамках Блока 1 «Дисциплины (модули)» реализуется дисциплина (модуль) «Физическая подготовка»:

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

в объеме не менее 328 академических часов, которые являются обязательными для освоения, не переводятся в з.е. и не включаются в объем программы базового высшего образования.

Программа специализированного высшего образования в рамках Блока 1 «Дисциплины (модули)» должна обеспечивать реализацию дисциплин (модулей), определенных Характеристикой образовательной программы.

2.7. При разработке и реализации образовательных программ обучающимся обеспечивается возможность освоения элективных дисциплин (модулей) и факультативных дисциплин (модулей). Факультативные дисциплины (модули) не включаются в объем образовательных программ.

2.8. В Блок 2 «Практика» входят по программам базового высшего образования учебная практика и производственная практика, по программам специализированного высшего образования – производственная практика (далее вместе – практики).

Типы учебной практики:

учебно-лабораторный практикум;

ознакомительная практика;

экспериментально-исследовательская практика.

Типы производственной практики:

технологическая практика;

проектно-технологическая практика;

эксплуатационная практика;

научно-исследовательская работа;

преддипломная практика.

Преддипломная практика проводится для выполнения выпускной квалификационной работы и является обязательной.

Организация:

выбирает один или несколько типов учебной практики (для программ базового высшего образования) и один или несколько типов производственной практики из перечня, указанного в настоящем пункте;

вправе установить дополнительный тип (типы) практик;

устанавливает объемы практик каждого типа;

устанавливает способ проведения каждой практики.

При реализации образовательной программы Организация осуществляет проведение практик в организациях, деятельность которых соответствует направленности (профилю, специализации) образовательной программы, или в структурных подразделениях Организации, предназначенных для проведения практической подготовки выпускников.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, за счет времени, выделяемого на проведение практик, могут проводиться комплексные учения (специальные профессиональные деловые игры).

2.9. В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, особенности организации и продолжительность проведения практик, а также возможность освоения элективных дисциплин (модулей) и факультативных дисциплин (модулей) определяются в порядке организации и осуществления образовательной деятельности по образовательной программе, устанавливаемом федеральным государственным органом, в ведении которого находятся соответствующие организации[10].

2.10. В Блок 3 «Государственная итоговая аттестация» входят:

подготовка к сдаче и сдача государственного экзамена (если Организация включила государственный экзамен в состав государственной итоговой аттестации);

подготовка к процедуре защиты и защита выпускной квалификационной работы.

2.11. В рамках образовательных программ Организацией выделяются обязательная часть и часть, формируемая участниками образовательных отношений.

В обязательную часть образовательных программ включаются:

Блок 2 «Практика»;

Блок 3 «Государственная итоговая аттестация»;

дисциплины (модули), указанные в пункте 2.6 настоящего ФГОС ВО.

[10] Часть 2 статьи 81 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (Собрание законодательства Российской Федерации, 2012, № 53, ст. 7598; 2016, № 27, ст. 4238).

Дисциплины (модули), входящие в Блок 1 «Дисциплины (модули)», за исключением дисциплин (модулей), указанных в пункте 2.6 настоящего ФГОС ВО, могут включаться в обязательную часть образовательных программ и (или) в часть, формируемую участниками образовательных отношений.

Объем обязательной части образовательной программы должен составлять не менее:

Программа базового высшего образования со сроком обучения 5 – 5,5 лет	**Программа специализированного высшего образования**
70 %	30 %

2.12. Реализация части (частей) образовательной программы, в рамках которой (которых) до обучающихся доводятся сведения ограниченного доступа и (или) в учебных целях используются секретные образцы вооружения, военной техники, их комплектующие изделия, а также проведение государственной итоговой аттестации не допускаются с применением электронного обучения, дистанционных образовательных технологий.

2.13. Объем образовательной программы в форме контактной работы обучающихся с педагогическими работниками Организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (в том числе с применением дистанционных образовательных технологий) в целом по Блоку 1 «Дисциплины (модули) от общей трудоемкости дисциплин в часах должен составлять не менее:

Форма обучения	**Программа базового высшего образования со сроком обучения 5 – 5,5 лет**	**Программа специализированного высшего образования**
очная	50 %	45 %
очно-заочная	35 %	30 %

2.14. Организация должна предоставлять инвалидам и лицам с ОВЗ (по их заявлению) возможность обучения по образовательным программам, учитывающим особенности их психофизического развития, индивидуальных возможностей и, при необходимости, обеспечивающей коррекцию нарушений развития и социальную адаптацию указанных лиц.

X. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ВОСПИТАНИЯ ОБУЧАЮЩИХСЯ ПРИ РЕАЛИЗАЦИИ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

x.1. Образовательные организации самостоятельно разрабатывают рабочую программу воспитания и календарный план воспитательной работы при разработке

образовательных программ базового высшего образования[11], которые направлены на формирование следующих духовно-нравственных ценностей:

верность Конституции Российской Федерации, гражданственность;

патриотизм, служение Отечеству и ответственность за его судьбу;

уважение и соблюдение прав и свобод человека и гражданина;

приверженность традиционным семейным ценностям, крепкая семья;

приоритет духовного над материальным, созидательный труд;

коллективизм, взаимопомощь и взаимоуважение;

гуманизм, милосердие, справедливость;

историческая память и преемственность поколений, единство народов России.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

3.1. При разработке образовательных программ Организация формирует требования к результатам их освоения в виде компетенций выпускников следующих видов:

универсальные компетенции (для программ базового высшего образования);

базовые компетенции (на УГСН);

общепрофессиональные компетенции (по специальности или направлению подготовки);

профессиональные компетенции (по конкретной образовательной программе).

3.2. Образовательные программы базового высшего образования должны устанавливать следующие универсальные компетенции и результаты обучения по их достижения (далее – УК):

Код УК	Формулировка компетенции	Результаты обучения по достижению компетенции	
		знать	уметь
Наименование категории УК – Ценности и мировоззрение, научная методология и системное мышление			
УК-1	Способен использовать философские знания, научную методологию и традиционные духовно-нравственные ценности для формирования научного мировоззрения, логического и системного мышления	Основные направления зарубежной и отечественной философии. Принципы и категории диалектики, формально-логические законы, принципы и приемы системного и критического мышления. Методологию научного познания и методы анализа социальных процессов. Традиционные духовно-нравственные ценности и мировоззренческие основы российского общества.	Применять знания о традиционных духовно-нравственных ценностях, логические законы, методы и приемы системного и критического мышления в социальной и профессиональной деятельности в целях, выявления тенденций социальной действительности, определения целей и методов в научном исследовании.

[11] Подпункт 1, 2 статья 12.1 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (Собрание законодательства Российской Федерации, 2012, № 53, ст. 7598; 2018, № 32, ст. 5110). С учетом Указа Президента Российской Федерации от 09.11.2022 № 809.

Наименование категории УК – Историческое сознание и патриотизм			
УК-2	Способен анализировать основные этапы и закономерности исторического развития России, понимать ее место и роль в современном мире для формирования собственной гражданской позиции и развития патриотизма	Особенности, основные этапы и закономерности цивилизационного развития России, ее позитивную роль в мировой политике. Исторические и культурные основы единства многонационального народа России, ее национальные интересы. Основания общегражданской идентичности российского общества.	Анализировать основные этапы и закономерности развития России в контексте мировой истории. Обосновывать исторические завоевания, государственное, культурное, многонациональное и конфессиональное единство страны, общенациональные интересы и прогрессивную роль России в мировой политике и международных конфликтах. Критически осмысливать геополитическую ситуацию, аргументированно противодействовать фальсификациям российской истории.
Наименование категории УК – Правовое и политическое сознание, гражданская позиция			
УК-3	Способен формировать правовое сознание, отстаивать гражданскую позицию, в том числе нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению	Основные понятия права и государства. Основы государственно-политического устройства и законодательства России. Сущность коррупции, экстремизма и терроризма, их негативное влияние на социальные, экономические, политические и иные процессы.	Использовать правовые знания и нормы, знание истории российской государственности, функционирования ее политико-правовой системы для формирования правосознания и отстаивания гражданской позиции. Применять действующее законодательство в целях профилактики коррупционного поведения, проявлений экстремизма и терроризма, формирования нетерпимого отношения к ним. Выбирать правомерные формы взаимодействия с гражданами, структурами гражданского общества и органами государственной власти в типовых ситуациях.
Наименование категории УК – Саморазвитие и социальное взаимодействие			
УК-4	Способен осуществлять самоорганизацию, саморазвитие и социальное взаимодействие, достигать поставленных целей в командной работе	Методы самоорганизации и саморазвития. Ключевые правила социального, группового и командного взаимодействия, в том числе с нозологическими группами инвалидов. Основы принятия управленческих решений. Способы постановки индивидуальных и групповых задач.	Применять методы самоорганизации и индивидуального саморазвития. Создавать систему мотивации для достижения поставленных целей и выстраивать конструктивные отношения внутри коллектива и между командами.
Наименование категории УК – Коммуникация			
УК-5	Способен осуществлять деловую коммуникацию в устной и письменной формах	Правила и нормы деловой коммуникации	Вести дискуссию, выстраивать аргументацию в ходе деловой коммуникации.

	на государственном языке Российской Федерации и иностранном(ых) языке(ах).	на государственном и иностранном(ых) языках. Культурные нормы общения, методы аргументации и убеждения в процессе коммуникации.	Читать и переводить тексты по профессиональной тематике на иностранном(ых) языке(ах).
Наименование категории УК – Безопасность жизнедеятельности			
УК-6	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	Основные техносферные опасности, их свойства и характеристики, характер воздействия вредных и опасных факторов на человека и природную среду, методы защиты от них. Приемы оказания первой медицинской помощи	Применять методы и средства защиты человека и природной среды от воздействия вредных и опасных факторов. Оказывать первую медицинскую помощь
Наименование категории УК – Здоровьесбережение			
УК-7	Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной жизнедеятельности	Нормы здорового образа жизни и технологии сбережения здоровья в различных жизненных ситуациях и в профессиональной деятельности.	Планировать и реализовывать процесс физического самосовершенствования для обеспечения полноценной социальной и профессиональной деятельности.
Наименование категории УК – Экономическая культура и финансовая грамотность			
УК-8	Способен принимать обоснованные экономические и финансовые решения	Базовые принципы функционирования экономики. Факторы устойчивого социально-экономического и технологического развития общества, включая предпринимательство. Роль государства в создании общественных благ, понятие бюджетной системы, цели, задачи, последствия социально-экономической политики государства. Технологию формирования бизнес-проекта и финансово-экономического обоснования.	Использовать информацию об изменениях в экономике, в том числе перспективах социально-экономического и технического развития страны, последствиях социально-экономической политики при принятии экономических решений. Разрабатывать типовые варианты бизнес-проекта и финансово-экономического обоснования.

3.3. Образовательные программы должны устанавливать следующие базовые компетенции и результаты обучения по их достижению (далее – БК) единые для УГСН 34 «Информационная безопасность»:

Код БК	Формулировка компетенции	Результаты обучения по достижению компетенции	
		знать	уметь
Программы базового высшего образования			
БК-1	Способен применять математические методы для решения задач профессиональной деятельности	Основные положения теории пределов числовых последовательностей и функций, теории числовых рядов. Основные понятия и теоремы дифференциального	Решать типовые задачи на вычисление пределов функций, дифференцирование и интегрирование, на разложение функций в ряды, производить исследование функций,

		исчисления функций одной и нескольких переменных. Основные положения интегрального исчисления: теории неопределенного интеграла, определенного интеграла Римана, несобственного интеграла, кратного интеграла Римана.	применять приложения дифференциального и интегрального исчисления.
		Основные понятия и теоремы теории обыкновенных дифференциальных уравнений.	Решать типовые дифференциальные уравнения.
		Основные положения и методы теории рядов и интеграла Фурье.	Применять аппарат теории рядов и интеграла Фурье для решения задач математического анализа.
		Основные приемы дифференцирования и интегрирования функций комплексного переменного.	Применять аппарат теории функций комплексного переменного, в том числе для решения задач в действительной области.
		Основные понятия и методы теории вероятностей. Основные числовые и функциональные характеристики распределений случайных величин. Основы теории цепей Маркова, основные виды и характеристики случайных процессов. Различные виды предельных теорем для последовательностей независимых одинаково распределенных случайных величин.	Применять основные модели и методы решения теоретико-вероятностных задач, в том числе применять аппарат вероятностных распределений случайных величин.
		Основные понятия математической статистики. Методы построения статистических оценок параметров и доверительных интервалов. Основные методы проверки статистических гипотез.	Строить статистические модели экспериментов, оценивать параметры статистических моделей, вычислять характеристики критериев проверки статистических гипотез.
		Основные понятия векторной алгебры и аналитической геометрии. Основные виды уравнений простейших геометрических объектов.	Решать типовые задачи аналитической геометрии.
		Основы теории матриц над полем. Основы теории линейных векторных пространств и их преобразований. Методы решений систем линейных уравнений над полем. Основы теории евклидовых пространств и их преобразований.	Решать типовые задачи линейной алгебры.

		Элементы комбинаторики, теории булевых функций, теории графов, теории конечных автоматов, теории кодирования.	Решать типовые задачи дискретной математики.
БК-2	Способен применять физические законы и модели для решения задач профессиональной деятельности	Основные законы механики. Основные законы термодинамики и молекулярной физики. Основные законы электричества и магнетизма. Основы теории колебаний и волн, волновой оптики. Основы квантовой физики.	Решать типовые физические задачи. Проводить эксперимент, обрабатывать и интерпретировать его результаты.
БК-3	Способен применять языки, методы и инструментальные средства программирования для решения задач профессиональной деятельности	Архитектуру и принципы работы вычислительных систем. Основные аппаратные компоненты вычислительных систем. Представление данных в памяти компьютера. Основные конструкции и библиотеки языка программирования. Принципы построения программ в различных парадигмах. Способы отладки и тестирования программного обеспечения. Основные структуры данных. Основные комбинаторные и теоретико-графовые алгоритмы. Основные алгоритмы сортировки и поиска.	Разрабатывать, отлаживать и тестировать программное обеспечение.
БК-4	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	Сущность и понятие информационной безопасности, характеристику ее составляющих. Сущность, понятие и классификация уязвимостей, угроз и атак на различные виды информационных систем. Основы государственной информационной политики и угрозы, связанные с развитием и повсеместным внедрением информационно-коммуникационных технологий. Назначение, структуру и состав системы обеспечения информационной безопасности Российской Федерации, ее место в системе национальной безопасности. Основные способы и средства обеспечения информационной безопасности,	Соотносить события окружающей действительности с угрозами информационной безопасности.

		принципы построения систем защиты информации. Основы обеспечения безопасности критической информационной инфраструктуры Российской Федерации, функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Основные приложения социальной инженерии в сфере защиты информации.	
БК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	Систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации. Систему международных и национальных стандартов в области защиты информации. Правовые основы организации защиты государственной тайны, иной информации ограниченного доступа. Систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию отдельных видов деятельности в области защиты информации, сертификации средств защиты информации и аттестации объектов информатизации. Меры административной и уголовной ответственности за правонарушения и преступления в области защиты информации. Задачи органов защиты государственной тайны и служб защиты информации на предприятиях (в организациях). Систему организационных мер, направленных на защиту информации ограниченного доступа.	Работать с правовой информационно-справочной системой. Разрабатывать локальные нормативные акты и методические документы по защите информации.
БК-6	Способен применять методы и средства криптографической защиты информации при решении задач профессиональной деятельности	Основные понятия криптографии и криптографические методы защиты информации. Основные криптографические алгоритмы и механизмы, определяемые межгосударственными стандартами	Осуществлять обоснованный выбор средств криптографической защиты информации для решения задач профессиональной деятельности. Применять в профессиональной деятельности типовые средства

		и национальными стандартами Российской Федерации, рекомендациями и техническими спецификациями Российской Федерации, стандартами международных организаций по стандартизации. Основные типы средств криптографической защиты информации и предъявляемые к ним требования.	криптографической защиты информации.
БК-7	***Способен применять средства защиты информации от утечки по техническим каналам*** ***(на обсуждение)***	*Технические каналы утечки информации. Методы, способы и средства защиты информации от утечки по типовым техническим каналам на объектах информатизации. Организацию защиты информации от утечки по техническим каналам на объектах информатизации.*	*Проводить предпроектное обследование объекта информатизации с целью выявления потенциальных технических каналов утечки информации. Обосновывать рациональный состав средств защиты информации от утечки по техническим каналам для защиты объекта информатизации. Устанавливать и настраивать типовые средства защиты информации от утечки по техническим каналам.*
Программы специализированного высшего образования			
БК-1	Способен разрабатывать проекты нормативных и организационно-распорядительных документов в области информационной безопасности, защиты информации	Нормативные правовые, методические документы ФСБ России, ФСТЭК России. Национальные стандарты в области защиты информации и информационной безопасности. Требования к содержанию организационно-распорядительных документов по обеспечению информационной безопасности.	Разрабатывать проекты нормативных и организационно-распорядительных документов по обеспечению информационной безопасности и защите информации.

3.4. Образовательные программы должны устанавливать общепрофессиональные компетенции и результаты обучения по их достижению в соответствии с Характеристикой образовательной программы.

3.5. Профессиональные компетенции и результаты обучения по их достижению определяются Организацией самостоятельно на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников (при наличии) (за исключением профессиональных компетенций по образовательным программам, указанным в пункте 1.13 ФГОС ВО), и (или) с учетом перспектив развития рынка труда, сферы профессиональной деятельности выпускников, а также приоритетов научно-технологического развития Российской Федерации.

Организация осуществляет выбор профессиональных стандартов, соответствующих профессиональной деятельности выпускников, из реестра профессиональных стандартов (перечня видов профессиональной деятельности), размещенного на специализированном сайте Министерства труда и социальной защиты Российской Федерации «Профессиональные стандарты» (http://profstandart.rosmintrud.ru) (при наличии соответствующих профессиональных стандартов).

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, перечень профессиональных компетенций, формируемых в рамках направленности (профиля, специализации), установленной в соответствии с пунктом 1.11 ФГОС ВО, определяется на основе анализа квалификационных требований к военно-профессиональной, специальной профессиональной подготовке выпускников, устанавливаемых федеральным государственным органом, в ведении которого находятся соответствующие организации.

3.6. При разработке образовательных программ Организация вправе дополнить набор результатов обучения по достижению универсальных, базовых и (или) общепрофессиональных компетенций с учетом направленности (профиля, специализации) образовательной программы, а также приоритетов научно-технологического развития Российской Федерации и плана мероприятий по реализации Стратегии научно-технологического развития Российской Федерации.

3.7. Организация самостоятельно планирует результаты обучения по дисциплинам (модулям) и практикам.

Совокупность компетенций, установленных образовательными программами, должна обеспечивать выпускнику способность осуществлять профессиональную деятельность не менее чем в одной области профессиональной деятельности и (или) сфере профессиональной деятельности, установленной в соответствующих Характеристиках образовательных программ.

4. ТРЕБОВАНИЯ К УСЛОВИЯМ РЕАЛИЗАЦИИ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ

4.1. Требования к условиям реализации образовательных программ включают в себя общесистемные требования, требования к материально-техническому и учебно-методическому обеспечению, требования к кадровым и финансовым условиям реализации образовательных программ, а также требования к применяемым механизмам оценки качества образовательной деятельности и подготовки обучающихся по образовательным программам.

4.2. Общесистемные требования к реализации образовательных программ.

4.2.1. Организация должна располагать на праве собственности и (или) ином законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием)

для реализации образовательных программ по Блоку 1 «Дисциплины (модули)», Блоку 2 «Практика», в части, касающейся требований к практической подготовке обучающихся при проведении практики в Организации, Блоку 3 «Государственная итоговая аттестация» в соответствии с учебным планом.

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

Электронная информационно-образовательная среда Организации должна обеспечивать:

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

- формирование электронного портфолио обучающегося, состав которого определяет Организация самостоятельно.

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих. Функционирование электронной информационно-образовательной среды должно обеспечивать соблюдение требований по информационной безопасности и соответствовать законодательству Российской Федерации[12].

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, формирование, использование и эксплуатация электронной информационно-образовательной среды, доступ обучающихся к электронной информационно-образовательной среде, а также к современным профессиональным базам данных и информационным справочным системам, к компьютерной технике, подключенной к локальным сетям и (или) сети «Интернет», организуются федеральным государственным органом, в ведении которого находятся соответствующие организации.

4.2.3. Организация должна предоставлять инвалидам и лицам с ограниченными возможностями здоровья (по их заявлению) возможность обучения по образовательным программам учитывающей особенности

[12] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2020, № 24, ст. 3751), Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2018, № 1, ст. 82).

их физического развития и, при возможности, обеспечивающей социальную адаптацию указанных лиц.

4.2.4. При реализации образовательной программы Организация определяет отдельную кафедру или иное структурное подразделение, деятельность которого непосредственно направлена на реализацию образовательных программ, отнесенных к УГСН 34 «Информационная безопасность».

4.3. Требования к материально-техническому и учебно-методическому обеспечению образовательных программ.

4.3.1. Помещения должны представлять собой учебные аудитории для проведения учебных занятий всех видов, предусмотренных образовательными программами, оснащенные оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей).

Допускается частичная замена оборудования его виртуальными аналогами, позволяющими обучающимся получать знания и формировать умения, предусмотренные образовательными программами.

4.3.2. Организация должна быть обеспечена необходимым комплектом лицензионного программного обеспечения и (или) свободно распространяемого программного обеспечения, отечественного и/или зарубежного производства (состав определяется в рабочих программах дисциплин (модулей, практик).

4.3.3. Электронная информационно-образовательная среда должна обеспечивать одновременный доступ к системе не менее 25 процентов обучающихся по образовательным программам.

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

4.3.4. Обучающимся должен быть обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей).

Доступ обучающихся к профессиональным базам данных и информационным справочным системам в федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, организуется федеральным государственным органом, в ведении которого находятся соответствующие организации.

4.3.5. При реализации образовательных программ, отнесенных к УГСН 34 «Информационная безопасность» Организация должна иметь:

аудиторию (помещение), аттестованную на соответствие требованиям о защите информации ограниченного доступа, для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну;

специальную библиотеку (библиотеку литературы ограниченного доступа), предназначенную для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа;

лаборатории и (или) специально оборудованные кабинеты (классы, аудитории), обеспечивающие практическую подготовку в соответствии с направленностью (профилем, специализацией) образовательной программы, которую она реализует.

Компьютерные (специализированные) классы и лаборатории (если в них предусмотрены рабочие места на базе вычислительной техники) должны быть оборудованы вычислительной техникой из расчета одно рабочее место на каждого обучающегося при проведении учебных занятий в данных классах (лабораториях).

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

Минимально необходимый для реализации образовательных программ перечень материально-технического обеспечения включает в себя специально оборудованные помещения для проведения учебных занятий в соответствии с Характеристикой образовательной программы, в том числе для всех программ базового высшего образования

лабораторию программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, программно-аппаратными комплексами защиты информации от несанкционированного доступа, включающими в том числе средства криптографической защиты информации, средствами дублирования и восстановления данных, средства доверенной загрузки;

специально оборудованные кабинеты (классы, аудитории):

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

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

4.4. Требования к кадровым условиям реализации образовательных программ.

4.4.1. Реализация образовательных программ обеспечивается педагогическими работниками Организации, а также лицами, привлекаемыми Организацией к реализации образовательных программам на иных условиях.

4.4.2. Квалификация педагогических работников Организации должна отвечать квалификационным требованиям, указанным в профессиональных стандартах (при наличии) и (или) в квалификационных справочниках.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, квалификационные характеристики должностей руководителей и педагогических работников высшего образования и дополнительного профессионального образования определяются нормативными правовыми актами, устанавливаемыми федеральным государственным органом, в ведении которого находятся соответствующие образовательные организации.

4.4.3. Доля педагогических работников Организации, участвующих в реализации образовательной программы и лиц, привлекаемых Организацией к реализации образовательных программам на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), ведущих научную и (или) учебно-методическую и (или) практическую работу, соответствующую профилю преподаваемой дисциплины (модуля), должна составлять:

Программа базового высшего образования	**Программа специализированного высшего образования**
Не менее 70 %	Не менее 80 %

4.4.4. Доля лиц, привлекаемых Организацией к реализации образовательной программы на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), являющихся работниками иных организаций, осуществляющими трудовую деятельность в профессиональной сфере, соответствующей профессиональной деятельности, к которой готовятся выпускники (иметь стаж работы в данной профессиональной сфере не менее 3 лет), должна составлять:

Программа базового высшего образования	**Программа специализированного высшего образования**
Не менее 3 %	Не менее 5 %

4.4.5. Доля педагогических работников Организации и лиц, привлекаемых к образовательной деятельности Организации на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), имеющих ученую степень (в том числе ученую степень, признаваемую

в Российской Федерации) и (или) ученое звание (в том числе ученое звание, признаваемое в Российской Федерации), должна составлять:

Программа базового высшего образования	**Программа специализированного высшего образования**
Не менее 55 %	Не менее 60 %

В реализации образовательной программы, отнесенной к УГСН 34 «Информационная безопасность», должен принимать участие минимум один педагогический работник Организации, имеющий ученую степень или ученое звание по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» или 1.2.4. «Кибербезопасность» или по научной специальности, соответствующей направлениям подготовки кадров высшей квалификации по программам подготовки научно-педагогических кадров в адъюнктуре, отнесенным к УГСН 34 «Информационная безопасность».

Общее руководство научным содержанием программы специализированного высшего образования, отнесенной к УГСН 34 «Информационная безопасность», должно осуществляться научно-педагогическим работником Организации, имеющим ученую степень (в том числе ученую степень, признаваемую в Российской Федерации), осуществляющим самостоятельные научно-исследовательские (творческие) проекты (участвующим в осуществлении таких проектов) по направлению подготовки, имеющим ежегодные публикации по результатам указанной научно-исследовательской (творческой) деятельности в ведущих отечественных рецензируемых научных журналах и изданиях, а также осуществляющим ежегодную апробацию результатов указанной научно-исследовательской (творческой) деятельности на национальных и международных конференциях.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, к педагогическим работникам с учеными степенями и (или) учеными званиями приравниваются преподаватели военно-профессиональных и специальных профессиональных дисциплин (модулей) без ученых степеней и (или) ученых званий, имеющие профильное высшее образование, опыт военной службы (службы в правоохранительных органах) в области и с объектами профессиональной деятельности, соответствующими образовательной программе, не менее 10 лет, воинское (специальное) звание не ниже «майор» («капитан 3 ранга»), а также имеющие боевой опыт или государственные (ведомственные) награды, или государственные (отраслевые) почетные звания, или государственные премии.

4.4.6. Максимальное число обучающихся, для которых один и тот же педагогический работник Организации является руководителем выпускной квалификационной работы, должно составлять:

Программа базового высшего образования	Программа специализированного высшего образования
Не более 7 обучающихся	Не более 5 обучающихся

4.5. Требования к финансовым условиям реализации образовательных программ.

4.5.1. Финансовое обеспечение реализации образовательных программ должно осуществляться в объеме не ниже значений базовых нормативов затрат на оказание государственных услуг по реализации образовательной программы и значений корректирующих коэффициентов к базовым нормативам затрат, определяемых Министерством науки и высшего образования Российской Федерации.

В Организации, в которой законодательством Российской Федерации предусмотрена военная или иная приравненная к ней служба, служба в правоохранительных органах, финансовое обеспечение реализации образовательной программы должно осуществляться в пределах бюджетных ассигнований федерального бюджета, выделяемых федеральному органу исполнительной власти, в ведении которого находится указанная Организация.

4.6. Требования к применяемым механизмам оценки качества образовательной деятельности и подготовки обучающихся по образовательным программам.

4.6.1. Качество образовательной деятельности и подготовки обучающихся по образовательным программам определяется в рамках системы внутренней оценки, а также системы внешней оценки в рамках государственного контроля качества образования.

4.6.2. В целях совершенствования образовательных программ Организация при проведении регулярной внутренней оценки качества образовательной деятельности и подготовки обучающихся по образовательным программам привлекает работодателей и (или) их объединения, иных юридических и (или) физических лиц, включая педагогических работников Организации.

В рамках внутренней системы оценки качества образовательной деятельности по образовательным программам обучающимся предоставляется возможность оценивания условий, содержания, организации и качества образовательного процесса в целом и отдельных дисциплин (модулей) и практик.

5. ХАРАКТЕРИСТИКИ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ВЫСШЕГО ОБРАЗОВАНИЯ, ОТНОСЯЩИХСЯ К УГСН 34 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

5.1. Характеристика образовательной программы базового высшего образования – программы по специальности 34.01 «Кибербезопасность»

5.1.1. Обучение по образовательной программе может осуществляться в очной форме.

Объем образовательной программы вне зависимости от применяемых образовательных технологий, реализации образовательных программ с использованием сетевой формы, реализации образовательных программ по индивидуальному учебному плану составляет 330 з.е.

Максимальный объем занятий обучающегося с применением электронного обучения, дистанционных образовательных технологий не должен превышать 25 процентов объема Блока 1 «Дисциплины (модули)».

5.1.2. Срок получения образования по образовательной программе (вне зависимости от применяемых образовательных технологий), включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 5,5 лет.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, срок обучения по образовательной программе в связи с продолжительностью каникулярного времени обучающихся[13] составляет не менее 5 лет.

5.1.3. Области профессиональной деятельности, в которых выпускники, освоившие образовательную программу, могут осуществлять профессиональную деятельность:

01 Образование и наука (в сфере научных исследований);

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

12 Обеспечение безопасности (в сфере компьютерных систем и сетей в условиях существования угроз их информационной безопасности);

сфера обороны и безопасности;

сфера правоохранительной деятельности.

[13] Пункт 1 статьи 30 Положения о порядке прохождения военной службы, утвержденного Указом Президента Российской Федерации от 16 сентября 1999 г. № 1237 «Вопросы прохождения военной службы» (Собрание законодательства Российской Федерации, 1999, № 38, ст. 4534; № 42, ст. 5008; 2000, № 16, ст. 1678; № 27, ст. 2819; 2003, № 16, ст. 1508; 2006, № 25, ст. 2697; 2007, № 11, ст. 1284; № 13, ст. 1527; № 29, ст. 3679; № 35, ст. 4289; № 38, ст. 4513; 2008, № 3, ст. 169, 170; № 13, ст. 1251; № 43, ст. 4919; 2009, № 2, ст. 180; № 18, ст. 2217; № 28, ст. 3519; № 49, ст. 5918; 2010, № 27, ст. 3446; 2011, № 4, ст. 572; № 13, ст. 1741; № 40, ст. 5532; 2012, № 2, ст. 244; № 29, ст. 4075; № 47, ст. 6457; 2013, № 7, ст. 633; № 13, ст. 1526; 2014, № 8, ст. 783).

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

При разработке образовательной программы Организация выбирает специализацию программы из следующего перечня:

специализация № 1 «Анализ безопасности информационных технологий»;

специализация № 2 «Математические методы и формальные модели кибербезопасности»;

специализация № 3 «Разработка защищенного (доверенного) программного обеспечения»;

специализация № 4 «Разработка средств защиты информации и мониторинга безопасности киберсреды»;

специализация № 5 «Безопасность информационных технологий объектов критической информационной инфраструктуры» (по отраслям);

специализация № 6 «Компьютерно-техническая экспертиза, расследование инцидентов информационной безопасности»;

специализация № 7 «Обнаружение и нейтрализация киберугроз, средства мониторинга киберсреды»;

специализация № 8 «Кибербезопасность роботизированных (беспилотных) систем»;

специализация № 9 «Безопасность технологий квантовых вычислений»;

специализация № 10 «Специальные технологии кибербезопасности».

Образовательная программа по специализации № 10 «Специальные технологии кибербезопасности» определяется квалификационными требованиями к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемыми федеральным государственным органом, в ведении которого находятся соответствующие Организации.

5.1.4. Структура и объем программы базового высшего образования:

Структура образовательной программы		**Объем образовательной программы и ее блоков в з.е.**
Блок 1	Дисциплины (модули)	Не менее 282
Блок 2	Практика	Не менее 27
Блок 3	Государственная итоговая аттестация	6 – 9
Итого		330

Образовательная программа должна обеспечивать реализацию дисциплин (модулей) по операционным системам, компьютерным сетям, системам управления базами данных, защите в операционных системах, защите информации от утечки по техническим каналам, основам построения защищенных компьютерных сетей, основам построения защищенных баз данных, криптографическим протоколам в рамках Блока 1 «Дисциплины (модули)».

5.1.5. Образовательная программа должна устанавливать следующие общепрофессиональные компетенции и результаты обучения по их достижению по специальности 34.01 «Кибербезопасность»:

Код ОПК	Формулировка ОПК	Результаты обучения по достижению компетенции	
		знать	уметь
ОПК-1	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития технологий киберсферы, электронной компонентной базы	Принципы работы элементов и функциональных узлов электронной аппаратуры. Типовые схемотехнические решения основных узлов и блоков электронной аппаратуры. Состав, назначение и принципы функционирования основных аппаратных компонентов компьютерных систем. Направления совершенствования аппаратного обеспечения компьютерных систем.	Проводить анализ архитектуры и структуры аппаратного обеспечения компьютерных систем.
		Тенденции развития технологий цифровой экономики.	Анализировать новые технологии цифровой экономики на предмет возможных киберугроз.
		Принципы построения систем передачи информации и типовые сигналы, используемые в системах электросвязи. Основы регулирования и стандартизации в области связи. Базовые телекоммуникационные технологии сетей связи. Основные стандарты, архитектуру и протоколы мультисервисных сетей связи.	Проводить анализ основных характеристик и возможностей телекоммуникационных сетей по передаче информации.
		Технические каналы утечки информации. Методы, способы и средства защиты информации от утечки по техническим каналам на объектах информатизации.	Анализировать и оценивать технические каналы утечки информации на объектах информатизации.
ОПК-2	Способен применять криптографические протоколы при решении задач профессиональной деятельности	Принципы классификации и построения криптографических протоколов, их защиты от возможных уязвимостей. Автоматизированные средства анализа криптографических протоколов. Криптографические хеш-функции. Алгоритмы формирования и проверки цифровой подписи. Криптографические протоколы аутентификации сторон. Базовые криптографические протоколы передачи и распределения ключей, протоколы выработки общего	Осуществлять обоснованный выбор криптографических протоколов при решении задач профессиональной деятельности. Применять в профессиональной деятельности типовые криптографические протоколы.

		ключа, схемы предварительного распределения ключей. Основные элементы инфраструктуры открытых ключей. Криптографические протоколы проводных и беспроводных систем связи и передачи данных, их возможные уязвимости. Криптографические протоколы финансовой криптографии, их возможные уязвимости.	
ОПК-3	Способен применять методы научных исследований при проведении разработок в области защиты информации	Основные этапы и методы научного исследования. Порядок подготовки, оформления и представления основных видов научных работ.	Выполнять исследовательскую (научную) работу, оформлять и представлять отчетные материалы по ее результатам.
ОПК-4	Способен администрировать операционные системы с учетом решения задач по защите информации, выполнять работы по восстановлению работоспособности системного программного обеспечения	Принципы построения и функционирования, примеры реализаций современных операционных систем. Основные архитектурные компоненты операционных систем. Особенности построения операционных систем мобильных устройств.	Выполнять установку операционных систем, применять средства их конфигурирования и администрирования.
		Основные виды и угрозы безопасности операционных систем. Защитные механизмы и средства обеспечения безопасности операционных систем. Методы и средства хранения и передачи аутентификационной информации в операционных системах. Средства конфигурирования и администрирования основных архитектурных компонентов современных операционных систем. Основные требования к подсистеме аудита и политике аудита операционных систем. Методы и средства восстановления работоспособности системного программного обеспечения.	Применять средства формирования и анализа политик безопасности современных операционных систем.
ОПК-5	Способен администрировать компьютерные сети и сетевые сервисы, контролировать корректность их функционирования	Принципы построения и функционирования локальных и глобальных компьютерных сетей. Основные аппаратные средства построения компьютерных сетей.	Проектировать структуру и архитектуру компьютерной сети.
		Основные протоколы локальных и глобальных компьютерных сетей. Основные прикладные сетевые сервисы	Администрировать основные прикладные сетевые сервисы, их встроенные средства защиты информации.

		и применяемые ими протоколы прикладного уровня.	
ОПК-6	Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации	Терминологию в области баз данных и принципы их построения. Функциональные возможности реляционных и нереляционных баз данных и систем управления базами данных. Язык запросов к базам данных, способы оптимизации выполнения запросов. Механизм транзакций и особенности его использования в различных базах данных. Особенности и проблемы многопользовательского доступа к базе данных.	Проектировать и администрировать базу данных.
		Угрозы безопасности баз данных. Основные критерии защищенности баз данных и методы оценивания их механизмов защиты. Механизмы обеспечения конфиденциальности, целостности и высокой доступности баз данных. Основные программные интерфейсы взаимодействия с базами данных. Особенности применения криптографической защиты в системах управления базами данных. Этапы проектирования системы защиты в системах управления базами данных.	Создавать дополнительные средства защиты баз данных.
ОПК-7	Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в киберсреде и проводить анализ их безопасности	Принципы разработки системного программного обеспечения. Основные программные интерфейсы операционных систем. Основные программные интерфейсы сетевого взаимодействия.	Разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред.
		Основные типы уязвимостей программных реализаций. Основные методы и средства анализа программных реализаций. Основные методы и средства защиты программного обеспечения. Основные методы и средства защиты и надежного уничтожения данных на носителях информации.	Разрабатывать и проводить анализ безопасности компонентов средств защиты информации в киберсреде.
ОПК-8	Способен проводить мониторинг	Основные понятия и определения, используемые при	Разрабатывать модели угроз и модели нарушителя

	работоспособности и анализ эффективности средств защиты информации в киберсреде	описании моделей безопасности компьютерных систем. Основные виды политик управления доступом и информационными потоками в компьютерных системах.	безопасности компьютерных систем.
		Технологии создания и распространения компьютерных вирусов. Принципы построения и особенности функционирования средств обнаружения и нейтрализации вредоносного программного обеспечения. Функциональные возможности и основные особенности систем обнаружения вторжений и систем обнаружения атак. Методики анализа эффективности средств защиты информации в киберсреде. Методики оценки рисков для систем защиты информации в киберсреде.	Использовать программные средства анализа защиты компьютерных систем.

5.1.6. Требования к материально-техническому и учебно-методическому обеспечению образовательной программы.

Минимально необходимый для реализации образовательной программы перечень материально-технического обеспечения включает в себя специально оборудованные помещения для проведения учебных занятий, в том числе лаборатории:

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

- электроники и схемотехники, оснащенную учебно-лабораторными стендами (программными средствами эмуляции) электронных схем, обеспечивающими измерение и визуализацию частотных и временных характеристик сигналов электронной и цифровой аппаратуры;

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

- безопасности компьютерных сетей, оснащенную стендами для изучения проводных и беспроводных компьютерных сетей, включающими абонентские устройства, коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, средства обнаружения компьютерных атак, средства анализа защищенности компьютерных сетей;

- защиты информации от утечки по техническим каналам, оснащенную специализированным оборудованием по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам;

для специализации № 10 «Специальные технологии кибербезопасности» также:

выделенное помещение (аудитория) для проведения учебных занятий, в ходе которых до обучающихся доводятся сведения, составляющие государственную тайну;

кабинет огневой подготовки;

аудитория тактико-специальной (военно-профессиональной, специальной профессиональной) подготовки;

тир (для стрельбы из табельного оружия).

Лаборатория программно-аппаратных средств защиты информации дополнительно оснащается средствами анализа программных реализаций, программно-аппаратными комплексами поиска и уничтожения остаточной информации.

5.2. Характеристика образовательной программы базового высшего образования – программы по специальности 34.02 «Информационная безопасность телекоммуникационных систем»

5.2.1. Обучение по образовательной программе может осуществляться в очной форме.

Объем образовательной программы вне зависимости от применяемых образовательных технологий, реализации образовательных программ с использованием сетевой формы, реализации образовательных программ по индивидуальному учебному плану составляет 330 з.е.

Максимальный объем занятий обучающегося с применением электронного обучения, дистанционных образовательных технологий не должен превышать 25 процентов объема Блока 1 «Дисциплины (модули)».

5.2.2. Срок получения образования по образовательной программе (вне зависимости от применяемых образовательных технологий), включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 5,5 лет.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, срок обучения по программе специалитета в связи с продолжительностью каникулярного времени обучающихся[13] составляет не менее 5 лет.

5.2.3. Области профессиональной деятельности, в которых выпускники, освоившие образовательную программу, могут осуществлять профессиональную деятельность:

01 Образование и наука (в сфере научных исследований);

06 Связь, информационные и коммуникационные технологии (в сфере разработки и обеспечения функционирования сетей электросвязи, средств и систем обеспечения защиты от несанкционированного доступа сетей электросвязи и циркулирующей в них информации);

12 Обеспечение безопасности (в сфере обеспечения функционирования и развития сетей связи специального назначения);

сфера обороны и безопасности;

сфера правоохранительной деятельности.

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

При разработке образовательной программы Организация выбирает специализацию программы из следующего перечня:

специализация № 1 «Мониторинг в телекоммуникационных системах»;

специализация № 2 «Системы представительской связи»;

специализация № 3 «Сети специальной связи»;

специализация № 4 «Системы и сети связи специального назначения»;

специализация № 5 «Системы специальной связи и информации для органов государственной власти»;

специализация № 6 «Информационная безопасность аэрокосмических телекоммуникационных систем»;

специализация № 7 «Разработка защищенных телекоммуникационных систем»;

специализация № 8 «Управление информационной безопасностью телекоммуникационных сетей и систем»;

специализация № 9 «Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте» (по видам);

специализация № 10 «Системы цифровой защищенной связи с подвижными объектами»;

специализация № 11 «Информационная безопасность квантовых коммуникаций»;

специализация № 12 «Контроль защищенности информации в телекоммуникационных системах».

Образовательные программы по специализациям № 1 «Мониторинг в телекоммуникационных системах», № 2 «Системы представительской связи», № 3 «Сети специальной связи», № 4 «Системы и сети связи специального назначения», № 5 «Системы специальной связи и информации для органов государственной власти» определяются квалификационными требованиями к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемыми федеральным государственным органом, в ведении которого находятся соответствующие Организации.

5.2.4. Структура и объем программы базового высшего образования:

Структура образовательной программы		**Объем образовательной программы и ее блоков в з.е.**
Блок 1	Дисциплины (модули)	Не менее 282
Блок 2	Практика	Не менее 27
Блок 3	Государственная итоговая аттестация	6 – 9
Итого		330

Образовательная программа должна обеспечивать реализацию дисциплин (модулей) по программно-аппаратным средствам защиты информации, защите информации от утечки по техническим каналам, информационным технологиям, сетям и системам передачи информации, электронике и схемотехнике, теории электросвязи, измерениям в телекоммуникационных системах, проектированию защищенных телекоммуникационных систем, моделированию защищенных телекоммуникационных сетей и систем в рамках Блока 1 «Дисциплины (модули)».

5.2.5. Образовательная программа должна устанавливать следующие общепрофессиональные компетенции и результаты обучения по их достижению по специальности 34.02 «Информационная безопасность телекоммуникационных систем»

Код ОПК	Формулировка ОПК	Результаты обучения по достижению компетенции	
		знать	уметь
ОПК-1	Способен применять для решения физико-технических задач в сфере информационной безопасности положения теорий в областях электрических цепей, электроники и схемотехники, радиотехнических сигналов, распространения радиоволн, кодирования, электрической связи, цифровой обработки сигналов	Устройство, принципы построения и работы, технические возможности и назначение, основные параметры и характеристики типовых электрических цепей. Методы анализа электрических цепей при постоянных напряжениях, гармонических и произвольных воздействиях.	Рассчитывать основные параметры типовых электрических цепей в стационарных и переходных режимах процессов в них. Производить оценку и измерение отдельных характеристик типовых электрических цепей.
		Принципы действия и характеристики электронных компонентов телекоммуникационных систем. Типовые схемотехнические решения основных узлов и блоков электронной аппаратуры. Методы анализа электрических схем. Основные правила выполнения и оформления электрических схем.	Анализировать элементную базу электронной аппаратуры. Работать с программными средствами схемотехнического моделирования и использовать измерительную технику при экспериментальном исследовании электронной аппаратуры.
		Основные математические модели, методы спектрального и корреляционного анализа сигналов, спектральные и корреляционные характеристики непрерывных и дискретных детерминированных сигналов. Основные виды модуляции сигналов.	Рассчитывать спектральные и корреляционные характеристики типовых детерминированных сигналов.

		Способы представления сообщений, сигналов и помех, преобразования сигналов в каналах связи. Основы оптимального приема сигналов в присутствии помех и типовые схемы оптимальных приемников.	Выбирать статистические модели сигналов и помех, типовые схемы оптимальных приемников и оценивать помехоустойчивость оптимального приема типовых сигналов на фоне помех.
		Основные понятия теории информации. Основные типы кодов источников информации и помехоустойчивых кодов, основные параметры и способы представления помехоустойчивых кодов.	Рассчитывать параметры помехоустойчивых кодов. Применять базовые способы кодирования и декодирования типовых помехоустойчивых кодов и кодов источников информации.
		Физические основы излучения и распространения радиоволн в различных средах, а также особенности распространения радиоволн различных диапазонов частот. Основные типы, принципы действия, характеристики и особенности антенн, линий передачи, элементов волноводной и фидерной техники, методы и приемы расчета их характеристик.	Рассчитывать параметры типовых трасс распространения радиоволн. Рассчитывать характеристики типовых антенн, линий питания и отдельных устройств СВЧ.
		Дискретные и цифровые сигналы и системы, способы их представления и описания, основные методы анализа дискретных сигналов и систем. Методы проектирования цифровых фильтров.	Применять методы анализа и синтеза цифровых сигналов и систем для решения задач профессиональной деятельности.
		Принципы построения и работы измерительных устройств и приборов. Методики обработки и оценки достоверности результатов измерений.	Проводить измерения в спектральной и временной областях.
ОПК-2	Способен применять информационные технологии, программные средства системного и прикладного назначений для решения задач профессиональной деятельности	Классификацию компьютерных систем, виды информационного взаимодействия и обслуживания, основы построения информационно-вычислительных систем. Назначение, функции и обобщённую структуру операционных систем, и типовые операционные системы. Типовые прикладные информационные технологии и программное обеспечение, используемое для решения задач профессиональной деятельности, включая	Применять выбранные информационные технологии, программные средства системного и прикладного назначений для решения задач профессиональной деятельности.

		системы баз данных, технологии распределенного реестра и искусственного интеллекта.	
ОПК-3	Способен применять технологии и технические средства сетей электросвязи, в том числе для создания и эксплуатации защищенных телекоммуникационных сетей и систем	Элементную базу телекоммуникационных систем, включая области применения и основные характеристики, принципы организации систем на кристалле. Основные архитектуры аппаратных средств телекоммуникационных систем и их отличия. Технологии аппаратной обработки «больших данных», построения распределенных систем и систем искусственного интеллекта, применяемые в защищенных телекоммуникационных системах.	Выбирать технологии и аппаратные средства телекоммуникационных систем и реализовывать на их основе отдельные узлы и устройства с учетом требований информационной безопасности.
		Состав и основные характеристики технических средств сетей электросвязи.	Эксплуатировать и настраивать типовые технические средства сетей электросвязи, проводить диагностику типовых неисправностей в работе средств связи сетей электросвязи и исправлять их.
ОПК-4	Способен применять программные, программно-аппаратные, технические средства защиты информации телекоммуникационных сетей и систем	Основные программные и программно-аппаратные средства защиты информации телекоммуникационных систем от несанкционированного доступа и принципы работы этих средств.	Настраивать типовые программные и программно-аппаратные средства защиты информации телекоммуникационных систем от несанкционированного доступа.
		Технические каналы утечки информации. Методы, способы и средства защиты информации от утечки по типовым техническим каналам на объектах информатизации.	Проводить предпроектное обследование объекта информатизации с целью выявления потенциальных технических каналов утечки информации. Обосновывать рациональный состав средств защиты информации от утечки по техническим каналам для защиты объекта информатизации. Устанавливать и настраивать средства защиты информации от утечки по техническим каналам.
ОПК-5	Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов	Эталонную модель взаимодействия открытых систем, основные протоколы и стандарты, используемые в сетях и системах электрической связи.	Оценивать технические возможности основных сетей и систем электрической связи как объектов защиты информации.

	информационно-телекоммуникационной, в том числе критической информационной инфраструктуры, с учетом обеспечения требований информационной безопасности	Основные сети и системы электрической связи, включая локальные и глобальные сети, сети «интернет вещей» и «промышленный интернет», системы квантового распределения ключей, принципы их построения и основные технические характеристики входящих в них элементов.	
		Способы выявления уязвимостей и типовые уязвимости элементов информационно-телекоммуникационной инфраструктуры. Принципы обеспечения информационной безопасности информационно-телекоммуникационной инфраструктуры. Основные угрозы безопасности информации и модели нарушителя, принципы формирования политики информационной безопасности телекоммуникационной системы. Типовые сценарии атак на элементы информационно-телекоммуникационной инфраструктуры. Организацию деятельности по обеспечению безопасности критической информационной инфраструктуры Российской Федерации. Основные требования, предъявляемые к организации защиты информации ограниченного доступа в процессе функционирования сетей электросвязи. Порядок организации защиты информации ограниченного доступа в процессе функционирования сетей электросвязи.	Выявлять уязвимости и анализировать угрозы информационно-телекоммуникационной инфраструктуре и циркулирующей в ней информации, выбирать необходимые средства для обеспечения информационной безопасности.
ОПК-6	Способен проводить инструментальный мониторинг качества обслуживания телекоммуникационных сетей и систем	Показатели качества обслуживания. Методики измерения и оценки параметров в телекоммуникационных сетях и системах.	Анализировать пропускную способность и предельную нагрузку сети связи, параметры передачи при прохождении по каналам связи.
ОПК-7	Способен проводить инструментальный анализ защищенности информации от	Типовые средства и методики для инструментальной оценки уровня защищённости	Проводить анализ защищенности информации от несанкционированного доступа

	несанкционированного доступа в телекоммуникационных сетях и системах для управления их функционированием	телекоммуникационных сетей и систем.	в телекоммуникационных сетях и системах.
ОПК-8	Способен формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование объектов, явлений и процессов защищенных телекоммуникационных систем, включая обработку и оценку достоверности их результатов	Принципы и основные этапы математического и имитационного моделирования, походы к формализации явлений и процессов телекоммуникационных систем, типовые модели объектов, явлений и процессов телекоммуникационных систем. Основные возможности избранного средства моделирования объектов, явлений и процессов телекоммуникационных систем.	Разрабатывать модели и проводить математическое и имитационное моделирование типовых объектов, явлений и процессов телекоммуникационных систем, в том числе защищенных телекоммуникационных систем.
ОПК-9	Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений на предмет обеспечения заданного уровня безопасности и требуемого качества обслуживания	Общие принципы проектирования сетей и систем электрической связи и принципы построения защищенных телекоммуникационных систем. Средства проектирования (прототипирования) защищенных телекоммуникационных систем. Номенклатуру и содержание нормативных правовых актов и нормативных методических документов, применяемых при проектировании защищенных телекоммуникационных систем. Состав технико-экономического обоснования проектируемых защищенных телекоммуникационных систем.	Разрабатывать необходимую техническую документацию в области проектирования защищенных телекоммуникационные систем с учетом действующих нормативных и методических документов. Проводить подготовку исходных данных для технико-экономического обоснования проектируемых защищенных телекоммуникационных систем. Анализировать проектные решения по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем. Проектировать элементы защищенных телекоммуникационных систем. Оформлять отчеты при проведении разработок в области функционирования, развития и обеспечения информационной безопасности телекоммуникационных сетей и систем.

5.2.6. Требования к материально-техническому и учебно-методическому обеспечению образовательной программы.

Минимально необходимый для реализации образовательной программы перечень материально-технического обеспечения включает в себя специально оборудованные помещения для проведения учебных занятий, в том числе лаборатории:

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

- электроники и схемотехники, оснащенную учебно-лабораторными стендами, средствами для измерения и визуализации частотных и временных характеристик сигналов, средствами для измерения параметров электрических цепей, средствами генерирования сигналов;

- цифровой обработки сигналов, оснащенную рабочими местами на базе вычислительной техники с поддержкой вычислений общего назначения на графических процессорах, платами цифровой обработки сигналов на базе сигнальных процессоров и программируемых логических интегральных схем, средствами разработки приложений для них;

- сетей и систем передачи информации, оснащенную рабочими местами на базе вычислительной техники, стендами сетей передачи информации с коммутацией пакетов и коммутацией каналов, структурированной кабельной системой, телекоммуникационным оборудованием, эмулятором активного сетевого оборудования, специализированным программным обеспечением для настройки телекоммуникационного оборудования;

- защиты информации от утечки по техническим каналам, оснащенную специализированным оборудованием по защите информации от утечки по акустическому, акустоэлектрическому каналам, каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам;

- измерений в телекоммуникационных системах, оснащенную рабочими местами на базе вычислительной техники, структурированной кабельной системой, стендами для исследования параметров сетевого трафика, элементами телекоммуникационных систем с различными типами линий связи (проводных, беспроводных), комплектом измерительного оборудования
для исследования параметров телекоммуникационных систем;

- моделирования и прототипирования защищенных телекоммуникационных сетей и систем, оснащенную рабочими местами на базе вычислительной техники, средствами моделирования и проектирования защищенных телекоммуникационных сетей и систем, средствами инструментального анализа защищенности информации от несанкционированного доступа в телекоммуникационных сетях и системах;

для специализаций № 1 «Мониторинг в телекоммуникационных системах», № 2 «Системы представительской связи», № 3 «Сети специальной связи», № 4 «Системы и сети

связи специального назначения», № 5 «Системы специальной связи и информации для органов государственной власти» также:

выделенное помещение (аудитория) для проведения учебных занятий, в ходе которых до обучающихся доводятся сведения, составляющие государственную тайну;

кабинет специальной техники, в том числе шифровальных средств;

кабинет огневой подготовки;

аудитория тактико-специальной (военно-профессиональной, специальной профессиональной) подготовки;

тир (для стрельбы из табельного оружия).

5.3. Характеристика образовательной программы базового высшего образования – программы по специальности 34.03 «Информационная безопасность автоматизированных систем»

5.3.1. Обучение по образовательной программе может осуществляться в очной форме.

Объем образовательной программы вне зависимости от применяемых образовательных технологий, реализации образовательных программ с использованием сетевой формы, реализации образовательных программ по индивидуальному учебному плану составляет 330 з.е.

Максимальный объем занятий обучающегося с применением электронного обучения, дистанционных образовательных технологий не должен превышать 25 процентов объема Блока 1 «Дисциплины (модули)».

5.3.2. Срок получения образования по образовательной программе (вне зависимости от применяемых образовательных технологий), включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 5,5 лет.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, срок обучения по образовательной программе в связи с продолжительностью каникулярного времени обучающихся[13] составляет не менее 5 лет.

5.3.3. Области профессиональной деятельности, в которых выпускники, освоившие образовательную программу, 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 и в других областях профессиональной деятельности при условии соответствия уровня их образования и полученных компетенций требованиям к квалификации работника.

При разработке образовательной программы Организация выбирает специализацию программы из следующего перечня:

специализация № 1 «Безопасность автоматизированных систем в кредитной-финансовой сфере»;

специализация № 2 «Безопасность автоматизированных систем на транспорте» (по видам);

специализация № 3 «Безопасность значимых объектов критической информационной инфраструктуры» (по отрасли или в сфере профессиональной деятельности);

специализация № 4 «Безопасность открытых информационных систем»;

специализация № 5 «Контроль защищенности автоматизированных систем»;

специализация № 6 «Проектирование автоматизированных систем в защищенном исполнении»;

специализация № 7 «Безопасность автоматизированных систем управления технологическими процессами» (по отрасли или в сфере профессиональной деятельности);

специализация № 8 «Мониторинг информационной безопасности автоматизированных систем»;

специализация № 9 «Информационная безопасность центров обработки данных, облачных и распределенных вычислительных сред»

специализация № 10 «Безопасность киберфизических систем»

специализация № 11 «Защита информации в автоматизированных информационных системах специального назначения».

Образовательная программа по специализации № 11 «Защита информации в автоматизированных информационных системах специального назначения» определяется квалификационными требованиями к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемыми федеральным государственным органом, в ведении которого находятся соответствующие Организации.

5.3.5. Структура и объем образовательной программы:

Структура образовательной программы		**Объем образовательной программы и ее блоков в з.е.**
Блок 1	Дисциплины (модули)	Не менее 282
Блок 2	Практика	Не менее 27
Блок 3	Государственная итоговая аттестация	6 – 9
Итого		330

Образовательная программа должна обеспечивать реализацию дисциплин (модулей) по сетям и системам передачи информации, программно-аппаратным средствам защиты информации, защите информации от утечки по техническим каналам, управлению информационной безопасностью, разработке и эксплуатации автоматизированных систем в защищенном исполнении в рамках Блока 1 «Дисциплины (модули)».

5.3.5. Образовательная программа должна устанавливать следующие общепрофессиональные компетенции и результаты обучения по их достижению по специальности 34.03 «Информационная безопасность автоматизированных систем»:

Код ОПК	Формулировка ОПК	Результаты обучения по достижению компетенции	
		знать	уметь
ОПК-1	Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	Основные этапы и методы научных исследований. Порядок подготовки, оформления и представления основных видов научных работ.	Оформлять и представлять отчетные материалы по итогам выполненной исследовательской (научной) работы. Применять методы и средства моделирования при проведении разработок в области защиты информации в автоматизированных системах.
ОПК-2	Способен применять информационные технологии, программные средства системного и прикладного назначения для решения задач профессиональной деятельности	Принципы построения и функционирования операционных систем, систем управления базами данных и компьютерных сетей. Порядок установки и первичной настройки операционных систем. Архитектуру и принципы проектирования реляционных и нереляционных баз данных. Архитектуру и принципы проектирования компьютерных сетей. Возможности информационных технологий для обеспечения безопасности автоматизированных систем.	Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети с учетом требований по обеспечению защиты информации автоматизированных.
ОПК-3	Способен решать задачи при администрировании информационной безопасности автоматизированных систем	Программные и программно-аппаратные средства и системы защиты информации автоматизированной системы. Порядок установки и настройки программных и программно-аппаратных средств защиты информации, используемых для обеспечения информационной безопасности	Проводить установку и настройку систем и средств защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией.

		автоматизированных систем.	
		Порядок организации технического обслуживания систем и средств защиты информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией.	Проводить техническое обслуживание систем и средств защиты информации автоматизированных систем в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией.
ОПК-4	Способен определять требования к обеспечению информационной безопасности на всех этапах жизненного цикла автоматизированной системы	Систему нормативных правовых актов и нормативных методических документов в области защиты информации. Основные категории информации, обрабатываемые в автоматизированных системах и требования по обеспечению их безопасности.	Формировать частные требования по обеспечению информационной безопасности в соответствии с категорией информации, обрабатываемой в автоматизированной системе, и требованиями нормативной базы.
		Основные этапы жизненного цикла автоматизированных систем и типовые угрозы информационной безопасности для каждого из них.	Формировать частные перечни угроз информационной безопасности для каждого этапа жизненного цикла автоматизированной системы.
		Основные угрозы безопасности информации в автоматизированной системе и негативные последствия, возникающих при их реализации. Основные модели нарушителя в автоматизированных системах. Организационные меры по защите информации в автоматизированной системе.	Разрабатывать в соответствии с методиками моделирования и иными нормативными документами модель угроз и нарушителя.
ОПК-5	Способен выявлять и устранять уязвимости системы защиты информации автоматизированных систем	Уязвимости общесистемного и специального программного обеспечения автоматизированных систем. Порядок проведения обследования автоматизированных систем на предмет наличия уязвимостей. Порядок построения центров мониторинга событий информационной безопасности. Порядок взаимодействия с центрами ГосСОПКА. Порядок расследования компьютерных инцидентов.	Проводить предварительное обследование автоматизированных систем на предмет наличия уязвимостей общесистемного и специального программного обеспечения.
		Содержание и порядок деятельности персонала по устранению уязвимостей систем защиты информации автоматизированных систем.	Устранять уязвимости систем защиты информации автоматизированных систем.

		Технические каналы утечки информации. Методы, способы и средства защиты информации от утечки по типовым техническим каналам на объектах информатизации.	Проводить предпроектное обследование объекта информатизации с целью выявления потенциальных технических каналов утечки информации. Обосновывать рациональный состав средств защиты информации от утечки по техническим каналам для защиты объекта информатизации. Устанавливать и настраивать средства защиты информации от утечки по техническим каналам.
ОПК-6	Способен осуществлять разработку и обоснование проектных решений по обеспечению информационной безопасности автоматизированных систем	Систему нормативных правовых актов и нормативных методических документов в области разработки автоматизированных систем и их систем защиты информации. Порядок формирования разделов технических заданий на создание систем обеспечения информационной безопасности автоматизированных систем. Методологию проектирования систем защиты информации автоматизированных систем. Порядок проведения оценки соответствия разработанных проектных решений требованиям по безопасности. Состав исходных данных для обоснования проектных решений по обеспечению информационной безопасности автоматизированных систем.	Проектировать системы защиты информации автоматизированных систем с учетом действующих нормативных правовых актов и нормативных методических документов.
ОПК-7	Способен осуществлять внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации	Систему нормативных правовых актов и нормативных методических документов в области эксплуатации автоматизированных систем. Основные категории мер по защите информации; компенсирующие меры по защите информации. Порядок и способы внедрения мер и средств по защите информации в автоматизированных системах.	Осуществлять выбор и внедрение мер и средств по защите информации в автоматизированные системы.
		Порядок проведения контроля защищенности систем защиты информации	Проводить контроль защищенности систем защиты информации

		автоматизированных систем.	автоматизированных систем.
ОПК-8	Способен реализовывать процессы управления информационной безопасностью автоматизированной системы	Обобщенные критерии и показатели обеспечения безопасности автоматизированных систем.	Разрабатывать критерии и показатели обеспечения безопасности автоматизированных систем.
		Типовые мероприятия по обеспечению безопасности автоматизированных систем.	Разрабатывать перечень мероприятий по обеспечению безопасности автоматизированных систем.
		Порядок осуществления контроля достижения показателей безопасности автоматизированных систем.	Осуществлять контроль достижения показателей безопасности автоматизированных систем.

5.3.6. Требования к материально-техническому и учебно-методическому обеспечению образовательной программы.

Минимально необходимый для реализации образовательной программы перечень материально-технического обеспечения включает в себя специально оборудованные помещения для проведения учебных занятий, в том числе лаборатории:

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

- сетей и систем передачи информации, оснащенную рабочими местами на базе вычислительной техники, стендами сетей передачи информации, проводных и беспроводных компьютерных сетей, включающих абонентские устройства, коммутаторы, маршрутизаторы, точки доступа, анализаторы кабельных сетей, средствами виртуализации сетей;

безопасности вычислительных сетей, оснащенную межсетевыми экранами, системами углубленной проверки сетевых пакетов, средствами организации безопасных виртуальных сетевых соединений, средствами анализа защищенности компьютерных сетей;

- защиты информации от утечки по техническим каналам, оснащенную специализированным оборудованием по защите информации от утечки по акустическому, акустоэлектрическому каналам, каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам;

- мониторинга защищенности автоматизированных систем, оснащенную аппаратно-программными средствами управления событиями информационной безопасности, средствами обнаружения вторжений, средствами анализа сетевого трафика, средствами мониторинга состояния автоматизированных систем;

для специализации № 11 «Защита информации в автоматизированных информационных системах специального назначения» также:

выделенное помещение (аудитория) для проведения учебных занятий, в ходе которых до обучающихся доводятся сведения, составляющие государственную тайну;

кабинет огневой подготовки;

аудитория тактико-специальной (военно-профессиональной, специальной

профессиональной) подготовки;

тир (для стрельбы из табельного оружия).

5.4. Характеристика образовательной программы базового высшего образования – программы по специальности 34.04 «Информационно-аналитические системы безопасности»

5.4.1. Обучение по образовательной программе может осуществляться в очной форме.

Объем образовательной программы вне зависимости от применяемых образовательных технологий, реализации образовательных программ с использованием сетевой формы, реализации образовательных программ по индивидуальному учебному плану составляет 330 з.е.

Максимальный объем занятий обучающегося с применением электронного обучения, дистанционных образовательных технологий не должен превышать 25 процентов объема Блока 1 «Дисциплины (модули)».

5.4.2. Срок получения образования по образовательной программе (вне зависимости от применяемых образовательных технологий), включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 5,5 лет.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, срок обучения по образовательной программе в связи с продолжительностью каникулярного времени обучающихся[13] составляет не менее 5 лет.

5.4.3. Области профессиональной деятельности, в которых выпускники, освоившие образовательную программу, могут осуществлять профессиональную деятельность:

01 Образование и наука (в сфере научных исследований);

06 Связь, информационные и коммуникационные технологии (в сфере разработки и системного анализа информационно-аналитических систем, автоматизации информационно-аналитической деятельности, защите информации в автоматизированных информационно-аналитических системах);

08 Финансы и экономика (в сфере финансового мониторинга противодействия легализации доходов, полученных преступным путем, и финансированию терроризма)

12 Обеспечение безопасности (в сфере разработки и эксплуатации информационно-аналитических систем безопасности);

сфера обороны и безопасности;

сфера правоохранительной деятельности.

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

При разработке образовательной программы Организация выбирает специализацию программы из следующего перечня:

специализация № 1 «Автоматизация информационно-аналитической деятельности»;

специализация № 2 «Информационная безопасность финансовых и экономических структур»;

специализация № 3 «Технологии информационно-аналитического мониторинга»;

специализация № 4 «Безопасность технологий больших данных»;

специализация № 5 «Информационная безопасность цифровых платформ социальной коммуникации»;

специализация № 6 «Математические методы компьютерной безопасности информационно-аналитических систем»;

специализация № 7 «Безопасность систем искусственного интеллекта»;

специализация № 8 «Конкурентный мониторинг и прогнозирование в киберсреде»;

специализация № 9 «Доверенные квантовые вычисления»;

специализация № 10 «Информационно-аналитические системы специального назначения».

Образовательная программа по специализации № 10 «Информационно-аналитические системы специального назначения» определяются квалификационными требованиями к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемыми федеральным государственным органом, в ведении которого находятся соответствующие Организации.

5.4.4. Структура и объем образовательной программы:

Структура образовательной программы		**Объем образовательной программы и ее блоков в з.е.**
Блок 1	Дисциплины (модули)	Не менее 282
Блок 2	Практика	Не менее 21
Блок 3	Государственная итоговая аттестация	6 – 9
Итого		330

Образовательная программа должна обеспечивать реализацию дисциплин (модулей) по безопасности информационно-аналитических систем, безопасности операционных систем, принципам построения, проектирования и эксплуатации информационно-аналитических систем, методам оптимизации, машинному обучению и нейронным сетям, обработке больших данных, методам анализа данных, распределенным информационно-аналитическим системам, моделированию информационно-аналитических систем в рамках Блока 1 «Дисциплины (модули)».

5.4.5. Образовательная программа должна устанавливать следующие общепрофессиональные компетенции и результаты обучения по их достижению по специальности 34.04 «Информационно-аналитические системы безопасности»:

Код ОПК	Формулировка ОПК	Результаты обучения по достижению компетенции	
		знать	уметь
ОПК-1	Способен разрабатывать и применять математические модели и методы и интерпретировать получаемые результаты	Основы теории погрешностей. Численные методы и алгоритмы решения задач профессиональной детальности.	Осуществлять выбор и применять численные методы и алгоритмы для решения задач профессиональной деятельности.
		Модели, методы и алгоритмы решения оптимизационных задач.	Решать оптимизационные задачи и интерпретировать профессиональный смысл получаемых формальных результатов.
		Методологические основы анализа данных. Методы анализа распределения данных. Методы анализа однородности данных. Методы анализа многомерных данных и снижения размерности.	Применять методы оценки зависимостей признаков, оценки смесей распределения, анализа главных компонент, факторного анализа и интерпретировать профессиональный смысл получаемых формальных результатов.
ОПК-2	Способен разрабатывать и применять методы и технологии искусственного интеллекта и машинного обучения для решения задач профессиональной деятельности	Постановки задачи, модели, методы и алгоритмы машинного обучения.	Применять методы машинного обучения для решения задач анализа массивов данных.
		Архитектуры искусственных нейронных сетей. Алгоритмы обучения искусственных нейронных сетей.	Применять модели и алгоритмы на основе искусственных нейронных сетей для решения задач профессиональной деятельности.
		Технологии интеллектуальной обработки и анализа текстовых данных. Технологии интеллектуальной обработки и анализа мультимедийных данных.	Применять алгоритмы и программные средства интеллектуальной обработки и анализа текстовых и мультимедийных данных.
ОПК-3	Способен разрабатывать и применять методы и технологии работы с большими данными для решения задач профессиональной деятельности	Основы сбора, обработки и анализа больших данных.	Применять методы и технологии сбора, обработки и анализа больших данных при решении задач профессиональной деятельности.
		Технологии хранения больших данных	Проектировать хранилища больших данных в системах управления данными различных типов: реляционные, колоночные, документальные, графовые и хранилищах типа «пара «ключ-значение».
ОПК-4	Способен применять экономические знания при решении задач обеспечения национальной безопасности	Национальные интересы и стратегические национальные приоритеты, угрозы экономической безопасности в различных сферах российского общества. Основные виды экономических преступлений	Анализировать экономическую информацию, применять результаты анализа в сфере обеспечения национальной безопасности.

		в финансовой, кредитно-банковской сфере и на рынке ценных бумаг.	
		Методы эконометрики и анализа временных рядов.	Решать эконометрические задачи и задачи прогнозирования временных рядов.
ОПК-5	Способен применять знания норм права при решении задач профессиональной деятельности	Систему нормативных правовых актов, нормативных и методических документов в области профессиональной деятельности. Правила применения норм материального и процессуального права при решении задач профессиональной деятельности.	Работать с правовой информационно-справочной системой. Применять нормы материального и процессуального права при решении задач профессиональной деятельности.
		Методы проведения предпроектного обследования, порядок документирования его результатов. Структуру и состав технического задания. Нормативно-методическую базу, регламентирующую процесс проектирования, информационно-аналитических систем.	Разрабатывать технические задания на создание автоматизированных информационно-аналитических систем, создавать проектные и организационно-распорядительные документы с учетом действующих нормативных и методических документов.
ОПК-6	Способен проектировать, настраивать, обслуживать основные компоненты функциональной и обеспечивающей частей информационно-аналитических систем, восстанавливать их работоспособность при возникновении внештатных ситуациях	Принципы оценки качества разрабатываемых информационно-аналитических систем. Методы проведения проверок функционирования информационно-аналитических систем. Принципы построения автоматизированных информационных систем.	Проводить содержательный анализ автоматизированных систем и исследовать проектные решения при их разработке.
		Методы, способы, средства, последовательность и содержание этапов проектирования автоматизированных систем.	Проектировать основные компоненты функциональной и обеспечивающей частей создаваемых информационно-аналитических систем.
		Классификацию методологий и средств компьютерной поддержки проектирования автоматизированных информационных систем.	Использовать технологии компьютерной поддержки проектирования в процессе разработки автоматизированных информационных систем.
		Основные меры защиты информации в автоматизированных системах.	
ОПК-7	Способен разрабатывать модели и оценивать эффективность информационно-аналитических систем	Методы построения и исследования аналитических и имитационных моделей процессов обработки информации в информационно-аналитических системах.	Строить и исследовать аналитические и имитационные модели процессов обработки информации в информационно-аналитических системах.

		Методы оценки эффективности процессов обработки информации в информационно-аналитических системах на базе математического моделирования.	Решать методами моделирования задачи исследования эффективности процессов обработки информации в информационно-аналитических системах.
ОПК-8	Способен обеспечивать выполнение требований информационной безопасности администрируемых операционных систем	Принципы построения современных операционных систем и особенности их применения. Основные модели управления доступом (дискреционная, мандатная, ролевая). Особенности управления доступом в современных операционных системах. Основные виды и угрозы безопасности операционных систем. Защитные механизмы и средства обеспечения безопасности операционных систем.	Настраивать компоненты защиты операционных систем.
ОПК-9	Способен обеспечивать выполнение требований информационной безопасности проектируемых баз данных, администрируемых вычислительных сетей, систем управления базами данных	Типовые угрозы безопасности баз данных. Штатные средства и методики обеспечения безопасности систем управления базами данных. Способы защиты баз данных от известных атак.	Пользоваться штатными средствами защиты информации, предоставляемыми системами управления базами данных.
		Основы организации и построения компьютерных сетей. Механизмы реализации атак в компьютерных сетях. Защитные механизмы и средства обеспечения сетевой безопасности.	Осуществлять основные меры противодействия нарушениям безопасности в компьютерных сетях.

5.4.6. Требования к материально-техническому и учебно-методическому обеспечению образовательной программы.

Минимально необходимый для реализации образовательной программы перечень материально-технического обеспечения включает в себя специально оборудованные помещения для проведения учебных занятий, в том числе

лаборатории:

- информационно-аналитических систем, оснащенным рабочими местами на базе вычислительной техники, с доступом к серверному оборудованию, позволяющим осуществлять высокопроизводительные, высоконагруженные, распределенные вычисления, хранение, дублирование и восстановление данных, а также средства мониторинга состояния вычислительной среды и средства визуализации коллективного пользования;

- искусственного интеллекта и машинного обучения, оснащенным рабочими

местами на базе вычислительной техники, с доступом к серверному оборудованию, позволяющему осуществлять высокопроизводительные вычисления с использованием графических процессоров, хранение, дублирование и восстановление данных;

специально оборудованный кабинет (класс, аудиторию) инструментальных средств программирования, оснащенный рабочими местами на базе вычислительной техники;

учебный ситуационный центр (полигон), оснащенный программно-аппаратным комплексом для хранения, обработки и анализа данных, средствами визуализации коллективного пользования и средствами поддержки принятия решений;

для специализации № 10 «Информационно-аналитические системы специального назначения» также:

выделенное помещение (аудитория) для проведения учебных занятий, в ходе которых до обучающихся доводятся сведения, составляющие государственную тайну;

кабинет огневой подготовки;

аудитория тактико-специальной (военно-профессиональной, специальной профессиональной) подготовки;

тир (для стрельбы из табельного оружия).

5.5. Характеристика образовательной программы базового высшего образования – программы по специальности 34.05 «Организация и технологии защиты информации»

5.5.1. Обучение по образовательной программе может осуществляться в очной и очно-заочной формах.

Объем образовательной программы вне зависимости от формы обучения, применяемых образовательных технологий, реализации образовательных программ с использованием сетевой формы, реализации образовательных программ по индивидуальному учебному плану составляет 300 з.е.

Максимальный объем занятий обучающегося с применением электронного обучения, дистанционных образовательных технологий не должен превышать 25 процентов объема Блока 1 «Дисциплины (модули)».

5.5.2. Срок получения образования по образовательной программе (вне зависимости от применяемых образовательных технологий) в очной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 5 лет.

5.5.3. Области профессиональной деятельности, в которых выпускники, освоившие образовательную программу, могут осуществлять профессиональную деятельность:

01 Образование и наука (в сфере научных исследований);

06 Связь, информационные и коммуникационные технологии (в сферах: защиты информации в организациях и на объектах информатизации);

12 Обеспечение безопасности в сфере обороны и правопорядка (в сфере правоохранительной деятельности);

сфера правоохранительной деятельности.

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

При разработке образовательной программы Организация выбирает специализацию программы из следующего перечня:

специализация № 1 «Техническая защита конфиденциальной информации»;

специализация № 2 «Организация и проведение компьютерных экспертиз»;

специализация № 3 «Организационно-правовое обеспечение защиты информации в организации»;

специализация № 4 «Организация защиты информации (по отраслям или в сфере профессиональной деятельности)»;

специализация № 5 «Технологии информационного противоборства в социотехнических системах;

специализация № 6 «Технологии защиты информации в правоохранительной сфере»;

специализация № 7 «Информационно-аналитическое обеспечение правоохранительной деятельности»;

специализация № 8 «Оперативно-техническое обеспечение раскрытия и расследования преступлений в сфере компьютерной информации».

Образовательные программы по специализациям № 6 «Технологии защиты информации в правоохранительной сфере», № 7 «Информационно-аналитическое обеспечение правоохранительной деятельности», № 8 «Оперативно-техническое обеспечение раскрытия и расследования преступлений в сфере компьютерной информации» определяются квалификационными требованиями к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемыми федеральным государственным органом, в ведении которого находятся соответствующие Организации.

Образовательные программы по специализациям № 1 «Техническая защита конфиденциальной информации», № 6 «Технологии защиты информации в правоохранительной сфере», № 7 «Информационно-аналитическое обеспечение правоохранительной деятельности», № 8 «Оперативно-техническое обеспечение раскрытия и расследования преступлений в сфере компьютерной информации» реализуется с соблюдением требований, предусмотренных законодательством Российской Федерации и иными нормативными правовыми актами в области защиты информации ограниченного доступа.

5.5.4. Структура и объем программы базового высшего образования:

Структура образовательной программы		Объем образовательной программы и ее блоков в з.е.
Блок 1	Дисциплины (модули)	Не менее 264
Блок 2	Практика	Не менее 24
Блок 3	Государственная итоговая аттестация	6 – 9
Итого		300

Образовательная программа должна обеспечивать реализацию дисциплин (модулей) по защите информации от утечки по техническим каналам, организации защиты информации в рамках Блока 1 «Дисциплины (модули)».

5.5.5. Образовательная программа должна устанавливать следующие общепрофессиональные компетенции и результаты обучения по их достижению по специальности 34.05 «Организация и технологии защиты информации»:

Код ОПК	Формулировка ОПК	Результаты обучения по достижению компетенции	
		знать	уметь
ОПК-1	Способен применять информационные технологии для решения профессиональных задач	Архитектура вычислительных систем. Основы построения вычислительных машин. Функциональная и структурная организация персонального компьютера.	Использовать персональные компьютеры для решения профессиональных задач.
		Общая характеристика операционных систем. Архитектура операционных систем.	Администрировать операционные системы.
		Основные модели данных. Системы управления базами данных. Организация баз данных. Организация доступа к данным.	Администрировать систему управления базами данных.
		Основы построения компьютерных сетей. Распределенная обработка данных. Протоколы связи. Технологии передачи данных.	Использовать вычислительные сети для решения профессиональных задач.
ОПК-2	Способен применять технологии поиска и анализа информации в профессиональной деятельности	Методы (технологии) обработки и анализа информации. Методы поиска информации. Современные информационные поисковые системы. Основы поиска информации в Интернет. Индексирование документов, основные электронные каталоги, библиотеки и базы данных, основные электронные ресурсы издательств.	Использовать информационные технологии для поиска и анализа информации. Работать с системами управления базами данных

		Основные специализированные базы данных и информационные ресурсы.	
ОПК-3	Способен применять для решения задач в сфере информационной безопасности положения теорий в областях электрических цепей и обработки сигналов	Устройство, основные параметры и характеристики типовых электрических цепей. Основные законы электрических цепей.	Рассчитывать основные параметры типовых электрических цепей. Проектировать и исследовать типовые электрические цепи в среде моделирования электронных схем.
		Основы аналого-цифрового и цифро-аналогового преобразования информации.	Проектировать и исследовать аналого-цифровые и цифро-аналоговые устройства в среде моделирования электронных схем.
ОПК-4	Способен применять программные, программно-аппаратные и технические средства защиты информатизации на объектах информатизации	Классификация и общая характеристика уязвимостей и угроз несанкционированного доступа к информации в автоматизированной системе. Модели нарушителя. Методика оценки угроз безопасности информации. Технологии аутентификации и идентификации. Модели управления доступом. Технологии обеспечения целостности и доступности данных. Угрозы безопасности вычислительных сетей, виды сетевых атак. Технологии защиты автоматизированных систем и вычислительных сетей от несанкционированного доступа к информации. Программные и программно-аппаратные средств защиты информации от несанкционированного доступа в автоматизированных системах. Антивирусные программы. Системы обнаружения и предупреждения сетевых вторжений.	Применять технологии аутентификации и идентификация для обеспечения безопасности автоматизированных систем и вычислительных сетей. Применять технологии управления доступом для обеспечения безопасности автоматизированных систем и вычислительных сетей. Применять технологии обеспечения целостности и доступности данных для обеспечения безопасности автоматизированных систем и вычислительных сетей. Проводить установку и настройку средств защиты информации от несанкционированного доступа в автоматизированных системах.
		Технические каналы утечки информации, обрабатываемой средствами вычислительной техники. Принципы построения и основные характеристики средств защиты объектов информатизации от утечки информации по техническим каналам.	Проводить анализ потенциальных технических каналов утечки информации на объектах информатизации. Проводить работы по установке и настройке средств защиты средств вычислительной техники от утечки информации по техническим каналам.

ОПК-5	Способен выполнять работы по созданию системы защиты информации на объекте информатизации	Нормативные правовые акты, методические и нормативные документы, национальные стандарты в области защиты информации (в том числе, ограниченного доступа) и аттестации объектов информатизации на соответствие требованиям по защите информации. Стандарты ЕСКД, ЕСТД и ЕСПД. Состав и порядок создания системы защиты информации на объектах информатизации. Уязвимости программных средств и систем, угрозы безопасности информации, обрабатываемой автоматизированной системой. Методика оценки угроз безопасности информации. Модель угроз безопасности информации. Меры (организационные, технические) по защите информации на объекте информатизации. Основные требования к системе защиты информации объекта информатизации. Содержание технического задания на создание системы защиты информации объекта информатизации.	Разрабатывать модель угроз безопасности информации объекта информатизации. Обосновывать технико-экономические требования к системе защиты информации на объекте информатизации. Разрабатывать техническое задание на создание системы защиты информации объекта информатизации.
ОПК-6	Способен организовывать и управлять мероприятиями по обеспечению информационной безопасности в организации	Организационные меры по защите информации, в том числе персональных данных. Основные методы управления защитой информации. Принципы организации защищенного документооборота в соответствии с требованиями законодательства. Принципы организации систем безопасности значимых объектов критической информационной инфраструктуры. Процедура категорирования объектов критической информационной инфраструктуры.	Разрабатывать предложения по совершенствованию процессов функционирования организации в целях обеспечения информационной безопасности. Организовывать мероприятия по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы организации и реагированию на компьютерные инциденты. Осуществлять планирование и организацию работы персонала с учетом требований по защите информации.
ОПК-7	Способен организовать эксплуатацию системы защиты информации на объекте	Нормативные правовые акты, методические и нормативные документы, национальные стандарты в области защиты информации (в том числе, ограниченного доступа) и аттестации	Разрабатывать организационно-распорядительные документы, определяющие мероприятия по защите информации на объекте информатизации. Организовать ввод в эксплуатацию системы защиты

		объектов информатизации на соответствие требованиям по защите информации. Состав и содержание эксплуатационной документации на систему защиты информации объекта информатизации. Состав и содержание организационно-распорядительных документов, определяющих мероприятия по защите информации на объекте информатизации. Порядок ввода системы защиты информации объекта информатизации в эксплуатацию. Основные этапы эксплуатации средств защиты информации, их краткая характеристика. Меры безопасности при эксплуатации средств защиты информации. Состав и содержание эксплуатационной документации на средства защиты информации.	информации объекта информатизации. Разрабатывать документы: по приему, выдаче, закреплению средств защиты информации, вводу средств защиты информации в эксплуатацию, выводу из эксплуатации и списанию средств защиты информации.
ОПК-8	Способен осуществлять контроль защищенности информации на объекте информатизации	Средства контроля защищенности информации в автоматизированной системе от несанкционированного доступа.	Проводить контроль защищенности автоматизированной системе на соответствие требованиям по защите информации от несанкционированного доступа.
		Аттестация объектов информатизации на соответствие требованиям о защите информации.	Организовать аттестацию объекта информатизации на соответствие требованиям о защите информации.

5.5.6. Требования к материально-техническому и учебно-методическому обеспечению образовательной программы.

Минимально необходимый для реализации образовательной программы перечень материально-технического обеспечения включает в себя специально оборудованные помещения для проведения учебных занятий, в том числе лаборатории:

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

- электроники, оснащенную учебно-лабораторными стендами, средствами для измерения и визуализации частотных и временных характеристик сигналов, средствами для измерения параметров электрических цепей, средствами генерирования сигналов, средствами для цифровой и аналоговой обработки сигналов;

- защиты информации от утечки по техническим каналам, оснащенную средствами защиты информации от утечки по каналам побочных электромагнитных излучений и

наводок, средствами защиты речевой акустической информации от утечки по акустическому, акустовибрационному и акустоэлектрическому каналам, средствами контроля средствами контроля защищенности информации от утечки по техническим каналам;

для специализаций № 6 «Технологии защиты информации в правоохранительной сфере», № 7 «Информационно-аналитическое обеспечение правоохранительной деятельности», № 8 «Оперативно-техническое обеспечение раскрытия и расследования преступлений в сфере компьютерной информации» также:

выделенное помещение (аудитория) для проведения учебных занятий, в ходе которых до обучающихся доводятся сведения, составляющие государственную тайну;

кабинет специальной техники и технических систем безопасности;

кабинет огневой подготовки;

кабинет тактико-специальной (военно-профессиональной, специальной профессиональной) подготовки;

тир (для стрельбы из табельного оружия).

5.6. Характеристика образовательной программы специализированного высшего образования – программы по направлению подготовки магистратуры 34.08 «Информационная безопасность»

5.6.1. Обучение по образовательной программе может осуществляться в очной и очно-заочной формах.

Объем образовательной программы вне зависимости от формы обучения, применяемых образовательных технологий, реализации образовательных программ с использованием сетевой формы, реализации образовательных программ по индивидуальному учебному плану составляет 120 з.е.

Максимальный объем занятий обучающегося с применением электронного обучения, дистанционных образовательных технологий не должен превышать 30 процентов объема Блока 1 «Дисциплины (модули)».

5.6.2. Срок получения образования по образовательной программе (вне зависимости от применяемых образовательных технологий) в очной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 2 года;

5.6.3. Области профессиональной деятельности, в которых выпускники, освоившие образовательную программу, могут осуществлять профессиональную деятельность:

01 Образование и наука (в сферах: профессионального образования и дополнительного профессионального образования; научных исследований, связанных с обеспечением информационной безопасности и защиты информации);

06 Связь, информационные и коммуникационные технологии (в сферах: защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи; технической защиты информации; защиты значимых объектов критической информационной инфраструктуры, информационно-аналитических систем безопасности);

12 Обеспечение безопасности (в сферах: обнаружения, предупреждения и ликвидации последствий компьютерных атак; противодействия иностранным техническим разведкам; технической защиты информации; криптографической защиты информации; обеспечения функционирования и развития сетей связи специального назначения; защиты значимых объектов критической информационной инфраструктуры, финансового мониторинга в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма);

сфера обороны и безопасности;

сфера правоохранительной деятельности.

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

5.6.4. Структура и объем образовательной программы:

Структура образовательной программы		**Объем образовательной программы и ее блоков в з.е.**
Блок 1	Дисциплины (модули)	Не менее 63
Блок 2	Практика	Не менее 39
Блок 3	Государственная итоговая аттестация	6 – 9
Итого		120

Образовательная программа должна обеспечивать реализацию дисциплин (модулей) по организации научных исследований, технологиям обеспечения информационной безопасности, управлению информационной безопасностью в рамках Блока 1 «Дисциплины (модули)».

5.6.5. Программа магистратуры должна устанавливать следующие общепрофессиональные компетенции и результаты обучения по их достижению по направлению 34.08 «Информационная безопасность»:

Код ОПК	Формулировка ОПК	Результаты обучения по достижению компетенции	
		знать	уметь
ОПК-1	Способен проводить научные исследования и разработки, включая сбор, обработку и анализ научно-технической	Основные этапы и методы проведения научного исследования. Методы обработки результатов исследования. Методику проведения патентных исследований.	Работать с источниками информации по теме научного исследования, систематизировать, классифицировать полученную информацию.

	информации, обработку результатов исследования, подготовку планов, научно-технических отчетов, научных докладов и статей	Правила и стандарты разработки отчетной документации, требования стандартов на оформление научно-технической документации.	Разрабатывать планы и программы проведения научных исследований и технических разработок. Оформлять результаты научных исследований в виде научно-технические отчетов, обзоров, научных докладов и статей. Представлять результаты научно-исследовательской деятельности в виде презентаций, устных докладов, вести научные дискуссии.
ОПК-2	Способен обосновывать требования к системе обеспечения информационной безопасности объектов информационной безопасности	Уязвимости объектов обеспечения информационной безопасности. Угрозы информационной безопасности. Особенности формирования системы обеспечения информационной безопасности. Процессы обеспечения информационной безопасности, включая процессы управления информационной безопасностью. Меры обеспечения информационной безопасности, реализующие процессы обеспечения информационной безопасности (организационные, технические). Процессы управления информационной безопасностью на этапах планирования, реализации, контроля и совершенствования системы обеспечения информационной безопасности. Нормативную и правовую базу в области обеспечения информационной безопасности, включая	Определять требования к обеспечению информационной безопасности. Проводить идентификацию активов объектов обеспечения информационной безопасности. Проводить анализ рисков информационной безопасности. Разрабатывать модели угроз и модели нарушителей информационной безопасности. Оценивать риски информационной безопасности. Выбирать процессы (включая процессы управления информационной безопасностью) и меры обеспечения информационной безопасностью. Формулировать положения политики обеспечения информационной безопасности. Разрабатывать техническое задание на создание систем обеспечения информационной безопасности.

		методические документы ФСБ России, ФСТЭК России и иных регуляторов.	
ОПК-3	Способен обосновывать требования к технологиям обеспечения информационной безопасности, используемым для обеспечения информационной безопасности конкретных объектов	Информационные технологии, используемые при построении объектов обеспечения информационной безопасности. Технологии обеспечения информационной безопасности, используемые для обеспечения состояния защищенности активов объектов обеспечения информационной безопасности и достижения необходимого качества обеспечения информационной безопасности.	Формулировать требования к технологиям обеспечения информационной безопасности, которые могут использоваться для обеспечения информационной безопасности конкретных объектов, использующих заданные информационные технологии. Обоснованно выбирать технологии обеспечения информационной безопасности, необходимые для обеспечения состояния защищенности активов объектов обеспечения информационной безопасности и достижения необходимого качества обеспечения информационной безопасности.

5.6.6. Требования к материально-техническому и учебно-методическому обеспечению образовательной программы.

Минимально необходимый для реализации образовательной программы перечень материально-технического обеспечения включает в себя специально оборудованные помещения для проведения учебных занятий, в том числе лабораторию в области технологий обеспечения информационной безопасности, оснащенную средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

5.7. Характеристика образовательной программы специализированного высшего образования – программы по направлению подготовки магистратуры 34.09 «Управление информационной безопасностью»

5.7.1. Обучение по образовательной программе может осуществляться в очной и очно-заочной формах.

Объем образовательной программы вне зависимости от формы обучения, применяемых образовательных технологий, реализации образовательных программ с

использованием сетевой формы, реализации образовательных программ по индивидуальному учебному плану составляет 60 з.е.

Максимальный объем занятий обучающегося с применением электронного обучения, дистанционных образовательных технологий не должен превышать 30 процентов объема Блока 1 «Дисциплины (модули)».

5.7.2. Срок получения образования по образовательной программе (вне зависимости от применяемых образовательных технологий) в очной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 1 год;

5.7.3. Области профессиональной деятельности, в которых выпускники, освоившие образовательную программу, могут осуществлять профессиональную деятельность:

06 Связь, информационные и коммуникационные технологии (в сферах: управления информационной безопасностью компьютерных систем и сетей, автоматизированных система систем и сетей электросвязи; значимых объектов критической информационной инфраструктуры);

12 Обеспечение безопасности (в сферах: обнаружения, предупреждения и ликвидации последствий компьютерных атак; противодействия иностранным техническим разведкам; технической защиты информации; криптографической защиты информации; обеспечения функционирования и развития сетей связи специального назначения; защиты значимых объектов критической информационной инфраструктуры, финансового мониторинга в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма);

сфера обороны и безопасности;

сфера правоохранительной деятельности.

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

5.7.4. Структура и объем образовательной программы:

Структура образовательной программы		**Объем образовательной программы и ее блоков в з.е.**
Блок 1	Дисциплины (модули)	Не менее 24
Блок 2	Практика	Не менее 21
Блок 3	Государственная итоговая аттестация	6
Итого		60

Образовательная программа должна обеспечивать реализацию дисциплин (модулей) по объектам автоматизированной обработки информации, процессам обеспечения информационной безопасности объектов автоматизированной обработки информации в рамках Блока 1 «Дисциплины (модули)».

5.7.5. Образовательная программа должна устанавливать следующие общепрофессиональные компетенции и результаты обучения по их достижению по направлению 34.09 «Управление информационной безопасностью»:

Код ОПК	Формулировка ОПК	Результаты обучения по достижению компетенции	
		знать	уметь
ОПК-1	Способен обосновывать требования к обеспечению информационной безопасности объектов автоматизированной обработки информации с учетом их особенностей и их роли при реализации основных процессов организации	Роль и место информационных технологий в процессах функционирования организации. Информационные технологии, используемые при построении объектов автоматизированной обработки информации. Особенности построения и функционирования объектов автоматизированной обработки информации. Особенности применения процессного подхода к описанию объектов автоматизированной обработки информации как части конкретной организации. Основные требования к обеспечению информационной безопасности объектов автоматизированной обработки информации.	Проводить обследование конкретного объекта автоматизированной обработки информации. Осуществлять идентификацию активов объектов автоматизированной обработки информации. Определять процессную модель организации и ее объектов автоматизированной обработки информации. Определять требования к обеспечению информационной безопасности объектов автоматизированной обработки информации.
ОПК-2	Способен применять процессный подход при обеспечении информационной безопасности конкретных объектов автоматизированной обработки информации	Уязвимости объектов автоматизированной обработки информации. Угрозы информационной безопасности объектов автоматизированной обработки информации. Особенности формирования системы обеспечения информационной безопасности объектов автоматизированной обработки информации. Процессы обеспечения информационной безопасности, входящие в системы обеспечения информационной безопасности объектов автоматизированной обработки информации, включая процессы защиты информации и процессы управления информационной безопасностью. Меры, реализующие процессы защиты информации и процессы управления информационной безопасностью. Процессы управления информационной безопасностью на этапах планирования, реализации, контроля и совершенствования системы обеспечения информационной безопасности объектов	Разрабатывать модели угроз информационной безопасности и модели нарушителей информационной безопасности конкретного объекта автоматизированной обработки информации. Выбирать процессы обеспечения информационной безопасности (включая процессы защиты информации и процессы управления информационной безопасностью) и меры, их реализующие, для системы обеспечения информационной безопасности конкретного объекта автоматизированной обработки информации. Формулировать положения политики обеспечения информационной безопасности конкретного объекта автоматизированной обработки информации. Осуществлять оценку информационной безопасности конкретного объекта автоматизированной обработки информации.

		автоматизированной обработки информации.	

5.7.6. Требования к материально-техническому и учебно-методическому обеспечению образовательной программы.

Минимально необходимый для реализации образовательной программы перечень материально-технического обеспечения включает в себя специально оборудованные помещения для проведения учебных занятий, в том числе лабораторию в области технологий обеспечения информационной безопасности, оснащенную средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.