Проект

Приложение

УТВЕРЖДЕН
приказом Министерства науки
и высшего образования
Российской Федерации
от «____»_____2023 г. №____

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] 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).

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, 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 обучения, дистанционных образовательных технологий не допускается[6].

Максимальный объем занятий обучающегося с применением

---

[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).

[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).

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

[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).

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 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

[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).

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.

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;

- 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.

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:

[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).

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

[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.

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.
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	Правила и нормы деловой коммуникации на государственном	Вести дискуссию, выстраивать аргументацию в ходе

	формах на государственном языке Российской Федерации и иностранном(ых) языке(ах).	и иностранном(ых) языках. Культурные нормы общения, методы аргументации и убеждения в процессе коммуникации.	деловой коммуникации. Читать и переводить тексты по профессиональной тема тике 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 исчисления функций одной и нескольких переменных. Основные положения интегрального исчисления: теории неопределенного интеграла, определенного интеграла Римана, несобственного интеграла, кратного интеграла Римана.	Решать типовые задачи на вычисление пределов функций, дифференцирование и интегрирование, на разложение функций в ряды, производить исследование функций, 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	Применять основные модели и методы решения теоретико-вероятностных задач, в том числе применять аппарат вероятностных

		распределений случайных величин. Основы теории цепей Маркова, основные виды и характеристики случайных процессов. Различные виды предельных теорем для последовательностей независимых одинаково распределенных случайных величин.	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	Решать типовые физические задачи. Проводить эксперимент, обрабатывать и интерпретировать его результаты.

		электричества и магнетизма. Основы теории колебаний и волн, волновой оптики. Основы квантовой физики.	
БК-3	Способен применять языки, методы и инструментальные средства программирования для решения задач профессиональной деятельности.	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. 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, принципы построения систем	Соотносить события окружающей действительности с угрозами информационной безопасности, представленными в документах стратегического планирования Российской Федерации.

		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.	
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	Работать с правовой информационно-справочной системой.

		государственной тайны и служб защиты информации на предприятиях (в организациях). Систему организационных мер, направленных на защиту информации ограниченного доступа.	
Программы специализированного высшего образования			
БК-1	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.	Нормативные и 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 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».

---

[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).

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.

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

---

[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).

специализацию программы из следующего перечня:

специализация № 1 «Анализ безопасности информационных технологий, тестирование на проникновение в киберсреде»;

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.	Проводить анализ основных характеристик и возможностей телекоммуникационных сетей по передаче информации.

		Базовые телекоммуникационные технологии сетей связи. Основные стандарты, архитектуру и протоколы мультисервисных сетей связи.	
		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 анализировать тенденции развития методов и средств криптографической защиты информации, применять 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 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.	Осуществлять обоснованный выбор средств криптографической защиты информации для решения задач профессиональной деятельности.
		Принципы классификации и построения криптографических протоколов, их защиты от возможных уязвимостей. Автоматизированные средства анализа криптографических протоколов. Криптографические хеш-функции.	Осуществлять обоснованный выбор криптографических протоколов при решении задач профессиональной деятельности.

		Алгоритмы формирования и проверки цифровой подписи. Криптографические протоколы аутентификации сторон. Базовые криптографические протоколы передачи и распределения ключей, протоколы выработки общего 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	Применять средства формирования и анализа политик безопасности современных операционных систем.

		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.	
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 и применяемые ими протоколы прикладного уровня.	Администрировать основные прикладные сетевые сервисы, их встроенные средства защиты информации.
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 работоспособности и анализ эффективности средств защиты информации в киберсреде.	Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем. Основные виды политик управления доступом	Разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем.

		и информационными потоками в компьютерных системах.	
		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,	Устройство, принципы построения и работы, технические возможности и назначение, основные параметры и характеристики типовых электрических цепей. Методы анализа электрических цепей при постоянных напряжениях,	Рассчитывать основные параметры типовых электрических цепей в стационарных и переходных режимах процессов в них. Производить оценку и измерение отдельных характеристик типовых электрических цепей.

	распространения радиоволн, кодирования, электрической связи, цифровой обработки сигналов.	гармонических и произвольных воздействиях.	
		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	Рассчитывать параметры помехоустойчивых кодов. Применять базовые способы кодирования и декодирования типовых помехоустойчивых кодов и кодов источников

		представления помехоустойчивых кодов.	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	Применять выбранные информационные технологии, программные средства системного и прикладного назначений для решения задач профессиональной деятельности.

		информационные технологии и программное обеспечение, используемое для решения задач профессиональной деятельности, включая системы баз данных, технологии распределенного реестра и искусственного интеллекта.	
ОПК-3	Способен применять технологии и технические средства сетей электросвязи, в том числе для создания 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, криптографические методы и средства защиты информации	Основные программные и программно-аппаратные средства защиты информации телекоммуникационных систем от несанкционированного доступа и принципы	Настраивать типовые программные и программно-аппаратные средства защиты информации телекоммуникационных систем от несанкционированного доступа.

	телекоммуникационных сетей и систем.	работы этих средств.	
		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.
		Основные понятия криптографии и криптографические методы защиты информации. Основные криптографические алгоритмы и механизмы, определяемые межгосударственными стандартами 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.	Осуществлять обоснованный выбор средств криптографической защиты информации для решения задач профессиональной деятельности.
ОПК-5	Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации	Эталонную модель взаимодействия открытых систем, основные протоколы и стандарты, используемые в сетях	Оценивать технические возможности основных сетей и систем электрической связи как объектов защиты информации.

	по построению элементов информационно-телекоммуникационной, в том числе критической информационной инфраструктуры, с учетом обеспечения требований информационной безопасности.	и системах электрической связи. 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,	Выявлять уязвимости и анализировать угрозы информационно-телекоммуникационной инфраструктуре и циркулирующей в ней информации, выбирать необходимые средства для обеспечения информационной безопасности.

		предъявляемые к организации защиты информации ограниченного доступа в процессе функционирования сетей электросвязи. Порядок организации защиты информации ограниченного доступа в процессе функционирования сетей электросвязи.	
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 несанкционированного доступа в телекоммуникационных сетях и системах для управления их функционированием	Типовые средства и методики для инструментальной оценки уровня защищённости телекоммуникационных сетей и систем.	Проводить анализ защищенности информации от несанкционированного доступа 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	Общие принципы проектирования сетей и систем электрической	Разрабатывать необходимую техническую документацию в области

	телекоммуникационные системы и их элементы, проводить анализ проектных решений на предмет обеспечения заданного уровня безопасности и требуемого качества обслуживания.	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.	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, 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 научного исследования. Порядок подготовки, оформления и представления основных видов научных работ.	Оформлять и представлять отчетные материалы по итогам выполненной исследовательской (научной) работы.
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	Программные и программно-аппаратные средства и системы защиты информации автоматизированной	Проводить установку и настройку систем и средств защиты информации автоматизированной системы в соответствии

	систем.	системы. Порядок установки и настройки программных и программно-аппаратных средств защиты информации, используемых для обеспечения информационной безопасности автоматизированных систем.	с ее эксплуатационной документацией.
		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 понятия криптографии и криптографические методы защиты информации. Основные криптографические алгоритмы и механизмы,	Осуществлять обоснованный выбор средств криптографической защиты информации для решения задач профессиональной деятельности.

		определяемые межгосударственными стандартами 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.	
		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.	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	Устранять уязвимости систем защиты информации автоматизированных систем.

		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	Проектировать системы защиты информации автоматизированных систем с учетом действующих нормативных правовых актов и нормативных методических документов.

		информационной безопасности автоматизированных систем.	
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 автоматизированных систем.	Проводить контроль защищенности систем защиты информации 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;

- 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	Решать оптимизационные задачи и интерпретировать

		оптимизационных задач.	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	Национальные интересы и стратегические национальные приоритеты, угрозы экономической	Анализировать экономическую информацию, применять результаты анализа в сфере обеспечения национальной

	безопасности.	безопасности в различных сферах российского общества. Основные виды экономических преступлений в финансовой, кредитно-банковской сфере и на рынке ценных бумаг.	безопасности.
		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,	Принципы оценки качества разрабатываемых информационно-аналитических систем. Методы проведения проверок функционирования информационно-аналитических систем. Принципы построения автоматизированных	Проводить содержательный анализ автоматизированных систем и исследовать проектные решения при их разработке.

	восстанавливать их работоспособность при возникновении внештатных ситуациях.	информационных систем.	
		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 применять 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 и национальными стандартами Российской Федерации, рекомендациями	Осуществлять обоснованный выбор средств криптографической защиты информации для решения задач профессиональной деятельности.

		и техническими спецификациями Российской Федерации, стандартами международных организаций по стандартизации. Основные типы средств криптографической защиты информации и предъявляемые к ним требования.	
ОПК-9	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-10	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	Использовать персональные компьютеры для решения профессиональных задач.

		компьютера.	
		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. Основные специализированные базы данных и информационные ресурсы.	Использовать информационные технологии для поиска и анализа информации. Работать с системами управления базами данных
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	Проектировать и исследовать аналого-цифровые и цифро-

		преобразования информации.	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.
		Основные понятия криптографии и криптографические методы защиты информации. Основные	Осуществлять обоснованный выбор средств криптографической защиты информации для решения задач профессиональной

		криптографические алгоритмы и механизмы, определяемые межгосударственными стандартами 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.	деятельности.
		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	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.

		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.	
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	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

		объектов критической информационной инфраструктуры.	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 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.	Разрабатывать организационно-распорядительные документы, определяющие мероприятия по защите информации на объекте информатизации. Организовать ввод в эксплуатацию системы защиты 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	Средства контроля защищенности	Проводить контроль защищенности

	контроль защищенности информации на объекте информатизации.	информации в автоматизированной системе от несанкционированного доступа.	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 информации, обработку результатов исследования, подготовку планов, научно-технических отчетов, научных докладов и статей.	Основные этапы и методы проведения научного исследования. Методы обработки результатов исследования. Методику проведения патентных исследований. Правила и стандарты разработки отчетной документации, требования стандартов на оформление научно-технической документации.	Работать с источниками информации по теме научного исследования, систематизировать, классифицировать полученную информацию. 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	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

		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 методические документы ФСБ России, ФСТЭК России и иных регуляторов.	(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.
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	Роль и место	Проводить обследование

	обосновывать требования к обеспечению информационной безопасности объектов автоматизированной обработки информации с учетом их особенностей и их роли при реализации основных процессов организации.	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.	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	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.

		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 автоматизированной обработки информации.	Формулировать положения политики обеспечения информационной безопасности конкретного объекта автоматизированной обработки информации. Осуществлять оценку информационной безопасности конкретного объекта 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.

Приложение

к федеральному государственному
образовательному стандарту
высшего образования по укрупненной группе
специальностей направлений подготовки
высшего образования
34 «Информационная безопасность»,
утвержденному приказом
Министерства науки и высшего образования
Российской Федерации
от «____»_____2023 г. №____

Перечень
специальностей базового высшего образования, после освоения которых возможно освоение программ специализированного высшего образования – программ магистратуры за счет средств федерального бюджета, бюджетов субъектов Российской Федерации и местных бюджетов

Код УГСН	Коды направлений	Наименования областей образования, УГСН и направлений. Наименование направлений
ИНЖЕНЕРНОЕ ДЕЛО, ТЕХНОЛОГИИ И ТЕХНИЧЕСКИЕ НАУКИ		
25	ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ	
	Все специальности и направления	
ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОМПЬЮТЕРНЫЕ НАУКИ		
32	ФУНДАМЕНТАЛЬНАЯ ИНФОРМАТИКА И МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ КОМПЬЮТЕРНЫХ НАУК	
	Все специальности и направления	
33	ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ	
	Все специальности и направления	
34	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ	
	Все специальности и направления	
ОБОРОНА И БЕЗОПАСНОСТЬ ГОСУДАРСТВА. ВОЕННЫЕ НАУКИ		
55	ВОЕННОЕ УПРАВЛЕНИЕ	
	06	Защита информации на объектах информатизации военного назначения