

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»



УТВЕРЖДАЮ

Ректор

В.Д. Нечаев

2022 г.

ПРИНЯТО

решением ученого совета
Севастопольского государственного
университета

«26» 05 2022 года

Протокол № 13

**ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
ВЫСШЕГО ОБРАЗОВАНИЯ**

Направление подготовки
10.03.01 Информационная безопасность

Профиль
Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)

Квалификация
бакалавр

Форма обучения, год набора
очная, 2022

Севастополь
2022

ЛИСТ СОГЛАСОВАНИЯ
Основной образовательной программы
высшего образования

Уровень высшего образования

бакалавриат

(название)

Направление подготовки

10.03.01 Информационная безопасность

(код и название)

Профиль

Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)

(название)

Квалификация

бакалавр

(название)

Проректор по образовательной деятельности


(подпись)

23.05.22
(дата)

В.Р. Душко

Директор Дирекции развития образовательных программ


(подпись)

16.05.22
(дата)

У.В. Дремова

И.о. директора Института радиоэлектроники и информационной безопасности


(подпись)

13.05.22
(дата)

С.Н. Девицына

РАЗРАБОТАНО

Руководитель образовательной программы

к.т.н., доцент, заведующий
кафедрой «Информационная
безопасность»

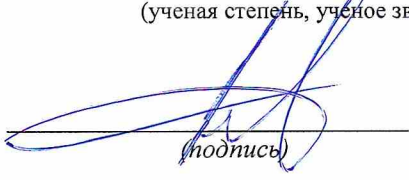
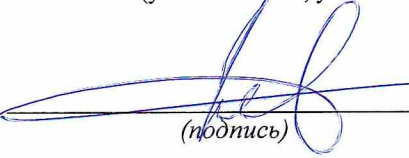
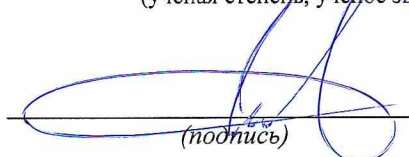

(подпись)

13.05.22
(дата)

М.И. Ожиганова

**Лист согласования основной образовательной программы
с представителями работодателей или их объединений
в соответствующей области профессиональной деятельности**

Основная образовательная программа высшего образования по направлению подготовки (специальности) 10.03.01 Информационная безопасность (направленность (профиль, специализация): Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности), 2022 год набора) соответствует требованиям федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427, отвечает требованиям профессиональных стандартов, соответствующих профессиональной деятельности выпускников, и требованиям к выпускникам на рынке труда.

	Рецензент (ведущий специалист – представитель работодателей или их объединений в соответствующей области профессиональной деятельности)
Основная образовательная программа по направлению подготовки 10.03.01 Информационная безопасность	<u>Начальник Управления защиты государственной тайны и мобилизационной работы Правительства г. Севастополя</u> (ученая степень, ученое звание, должность, место работы)  <u>В.С. Кобизской</u> (И.О. Фамилия)
Программа государственной итоговой аттестации по направлению подготовки 10.03.01 Информационная безопасность	<u>Начальник Управления защиты государственной тайны и мобилизационной работы Правительства г. Севастополя</u> (ученая степень, ученое звание, должность, место работы)  <u>В.С. Кобизской</u> (И.О. Фамилия)
Фонды оценочных средств государственной итоговой аттестации по направлению подготовки 10.03.01 Информационная безопасность	<u>Начальник Управления защиты государственной тайны и мобилизационной работы Правительства г. Севастополя</u> (ученая степень, ученое звание, должность, место работы)  <u>В.С. Кобизской</u> (И.О. Фамилия)

СОДЕРЖАНИЕ

1. Общие положения	5
1.1. Определение образовательной программы высшего образования по направлению подготовки 10.03.01 Информационная безопасность.	5
1.2. Нормативные документы для разработки ООП	5
1.3. Общая характеристика ООП	6
1.4. Требования к уровню подготовки, необходимому для освоения ООП	7
2. Характеристика профессиональной деятельности выпускников	9
2.1. Общее описание профессиональной деятельности выпускников	9
2.2. Перечень профессиональных стандартов, соотнесенных с ФГОС ВО	10
2.3. Перечень основных задач профессиональной деятельности выпускников	12
3. Планируемые результаты освоения ООП	14
4. Документы, регламентирующие структуру, содержание и организацию образовательного процесса при реализации ООП	39
4.1. Учебный план и календарный учебный график	39
4.2. Рабочие программы дисциплин (модулей)	40
4.3. Программы практик	40
4.4. Фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации	45
4.5. Программа государственной итоговой аттестации	45
4.6. Фонды оценочных средств государственной итоговой аттестации	45
5. Сведения об условиях реализации ООП	46
5.1. Общесистемное обеспечение реализации ООП	46
5.2. Кадровые условия реализации ООП	46
5.3. Материально-техническое и учебно-методическое обеспечение реализации ООП	47
5.4. Применяемые механизмы оценки качества образовательной деятельности и подготовки обучающихся	49
6. Рабочая программа воспитания	49
Приложение А. Аннотации к рабочим программам дисциплин	
Приложение Б. Рабочая программа воспитания	

1. Общие положения

1.1. Определение образовательной программы высшего образования по направлению подготовки 10.03.01 Информационная безопасность.

Основная образовательная программа высшего образования – программа бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (направленность (профиль): Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)) (далее – основная образовательная программа), реализуемая в федеральном государственном автономном образовательном учреждении высшего образования «Севастопольский государственный университет» (далее – Университет), представляет собой систему документов, разработанную с учетом потребностей регионального рынка труда, на основе федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427 (далее – федеральный государственный образовательный стандарт высшего образования).

Основная образовательная программа представляет собой комплекс основных характеристик образования (объем, содержание, планируемые результаты), организационно-педагогических условий, форм аттестации, который представлен в виде: учебного плана, календарного учебного графика, рабочих программ дисциплин (модулей), рабочих программ практик, программы государственной итоговой аттестации, рабочей программы воспитания, а также оценочных и методических материалов.

В настоящей программе используются следующие сокращения:

ЕГЭ – единый государственный экзамен;

НСД – несанкционированный доступ;

ООП – основная образовательная программа;

ОПК – общепрофессиональные компетенции;

ПК – профессиональные компетенции;

СКЗИ – средства криптографической защиты информации.

СССЭ – средства связи сетей электросвязи;

УК – универсальные компетенции;

ФГОС ВО – федеральный государственный образовательный стандарт высшего образования;

1.2. Нормативные документы для разработки ООП

1.2.1. Настоящая основная образовательная программа разработана с учетом требований следующих нормативных правовых документов:

- Федерального Закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

- Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427, зарегистрированного в Минюсте России 18 февраля 2021 г., рег. № 62548;

- Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования России от 6 апреля 2021 г. № 245;

- Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры, утвержденного приказом Министерства образования и науки Российской Федерации от 29.06.2015 № 636 (в ред. приказа Минобрнауки России от 9 февраля 2016 г. № 86, от 27 марта 2020 г. № 490);

- Положения о практической подготовке обучающихся, утвержденного приказом

Министерства науки и высшего образования Российской Федерации от 05.08.2020 № 885, приказом Министерства просвещения Российской Федерации от 05.08.2020 № 390 (в ред. приказа Минобрнауки России № 1430, Минпросвещения России № 652 от 18 ноября 2020 г.);

- Положения о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования, утвержденного приказом Министерства образования и науки Российской Федерации от 27.11.2015 № 1383;

- Постановления Правительства РФ от 10 февраля 2014 № 92 «Об утверждении Правил участия объединений работодателей в мониторинге и прогнозировании потребностей экономики в квалифицированных кадрах, а также в разработке и реализации государственной политики в области среднего профессионального образования и высшего образования»;

- Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ (утвержденного приказом Минобрнауки России от 9 января 2014 г. № 2);

- Письма Министерства образования и науки РФ № 03-956 от 13.05.2010 г. «Разъяснения разработчикам основных образовательных программ для реализации федеральных государственных образовательных стандартов высшего профессионального образования».

1.2.2. Настоящая основная образовательная программа разработана с учетом требований устава Университета, Положения о порядке разработки и утверждения основной образовательной программы № 42-01-09/74, принятого решением ученого совета Севастопольского государственного университета (протокол № 3/2019 от 18.11.2019) и утвержденного приказом ректора от 21.11.2019 № 1957-п, иных локальных нормативных актов, действующих в Университете.

1.3. Общая характеристика ООП

Форма обучения очная

Срок освоения ООП 4 года

Профиль подготовки Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Главной целью основной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность является развитие у студентов личностных качеств, формирование универсальных, общепрофессиональных и профессиональных компетенций для решения задач эксплуатационной, проектно-технологической, экспериментально-исследовательской и организационно-управленческой деятельности в соответствии с требованиями федерального государственного стандарта и достижениями науки и техники в области информационной безопасности.

Миссия (социальная значимость) основной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность состоит в концептуальном обосновании, моделировании современных условий и обеспечении подготовки высокопрофессиональных бакалавров, способных эффективно, с использованием фундаментальных теоретических и прикладных знаний и инновационных технологий осуществлять профессиональную деятельность в области информационной безопасности.

В области воспитания общей целью образовательной программы является создание условий по всестороннему развитию личности студентов, формирование социально-личностных и деловых качеств студентов: целеустремленности, организованности, трудолюбия, ответственности, гражданственности, коммуникативности, толерантности – позволяющих реализовать потенциал для решения профессиональных и социальных задач в профессиональной деятельности.

В области обучения общими целями образовательной программы по направлению подготовки 10.03.01 Информационная безопасность являются:

1) подготовка студентов в области основ гуманитарных, социальных, экономических, математических и естественнонаучных знаний и профессиональной деятельности;

2) получение высшего образования, позволяющего выпускнику успешно осуществлять решение задач профессиональной деятельности следующих типов:

- **эксплуатационный**: установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований; администрирование подсистем информационной безопасности объекта; участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

- **проектно-технологический**: сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности; проведение проектных расчетов элементов систем обеспечения информационной безопасности; участие в разработке технологической и эксплуатационной документации; проведение предварительного технико-экономического обоснования проектных расчетов;

- **экспериментально-исследовательский**: сбор и изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования; проведение экспериментов по заданной методике, обработка и анализ их результатов; проведение вычислительных экспериментов с использованием стандартных программных средств;

- **организационно-управленческий**: осуществление организационно-правового обеспечения информационной безопасности объекта защиты; организация работы малых коллективов исполнителей; участие в совершенствовании системы управления информационной безопасностью; изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа; контроль эффективности реализации политики информационной безопасности объекта защиты.

Согласно ФГОС ВО программа бакалавриата реализуется на государственном (русском) языке Российской Федерации, если иное не определено локальным нормативным актом Университета.

При успешном завершении обучения выпускнику присваивается квалификация «бакалавр» по специальности 10.03.01 Информационная безопасность.

После успешного завершения обучения и профессиональной адаптации бакалавры по направлению подготовки 10.03.01 Информационная безопасность должны достичь следующих профессионально-ориентированных целей:

1) формирование способностей к самосовершенствованию и профессиональному росту;

2) готовность к проектированию, разработке, эксплуатации и администрированию систем обеспечения информационной безопасности;

3) умение сочетать теоретические знания и практические навыки для решения профессиональных задач.

1.4. Требования к уровню подготовки, необходимому для освоения ООП

Требования к уровню подготовки, необходимому для освоения ООП определяются Правилами приема в ФГАОУ ВО «Севастопольский государственный университет» на обучение по программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (далее - Правила), ежегодно устанавливаемыми решением ученого совета Севастопольского государственного университета. Правила приема представлены на официальном сайте Университета в разделе сведения об образовательной организации (<https://www.sevsu.ru/sveden/document/>) (прямая ссылка на Правила приема 2022 г. <https://welcome.sevsu.ru/upload/iblock/708/708b5f7957d06cc4f3b93c605262a557.pdf>).

Прием на обучение по направлению подготовки 10.03.01 Информационная безопасность

проводится на первый курс на конкурсной основе (за исключением приема лиц, имеющих право на прием на обучение без вступительных испытаний):

- на базе среднего общего образования – на основании оцениваемых по стобалльной шкале результатов ЕГЭ, которые признаются в качестве результатов вступительных испытаний, и (или) по результатам вступительных испытаний, проводимых СевГУ самостоятельно в случаях, установленных Правилами;

- на базе среднего профессионального или высшего образования – по результатам общеобразовательных вступительных испытаний, проводимых СевГУ самостоятельно, либо одного или нескольких указанных вступительных испытаний наряду с использованием результатов ЕГЭ в качестве результатов других общеобразовательных вступительных испытаний, либо по результатам ЕГЭ в качестве результатов всех общеобразовательных вступительных испытаний.

Перечень вступительных испытаний (ЕГЭ):

- математика (профильная);
- информатика и ИКТ / физика / иностранный язык / химия;
- русский язык.

Для общеобразовательного вступительного испытания в качестве минимального количества баллов СевГУ используется минимальное количество баллов ЕГЭ:

- математика – 40 баллов;
- информатика и ИКТ – 45 баллов;
- физика – 40 баллов;
- иностранный язык – 30 баллов;
- химия – 40 баллов;
- русский язык – 40 баллов.

Конкурсный балл определяется как сумма баллов за каждое вступительное испытание (ЕГЭ), а также за индивидуальные достижения.

В соответствии с положениями главы IV Правил приема в ФГАОУ ВО «Севастопольский государственный университет» на обучение по образовательным программам высшего образования в 2022 году отдельным категориям поступающих, имеющих высокие результаты в учебе и спорте, предоставляются права поступления без вступительных испытаний, быть приравненным к лицам, набравшим максимальное количество баллов ЕГЭ по общеобразовательному предмету, соответствующему профилю олимпиады школьников, или к лицам, успешно прошедшим дополнительные вступительные испытания профильной, творческой и (или) профессиональной направленности.

Поступающему начисляются дополнительные баллы за следующие индивидуальные достижения:

- 1) наличие статуса чемпиона, призёра Олимпийских игр, Паралимпийских игр, Сурдлимпийских игр, чемпиона мира, чемпиона Европы, лица, занявшего первое место на первенстве мира, первенстве Европы по видам спорта, включенным в программы Олимпийских игр, Паралимпийских игр и Сурдлимпийских игр – 10 баллов;

- 2) наличие статуса чемпиона мира, чемпиона Европы, победителя первенства мира, первенства Европы по видам спорта, не включенным в программы Олимпийских игр, Паралимпийских игр и Сурдлимпийских игр – 10 баллов;

- 3) наличие золотого знака отличия Всероссийского физкультурно-спортивного комплекса "Готов к труду и обороне" (ГТО) и удостоверения к нему установленного образца, полученных в текущем или предшествующем году – 4 балла;

- 4) наличие серебряного или бронзового знака отличия Всероссийского физкультурно-спортивного комплекса "Готов к труду и обороне" (ГТО) и удостоверения к нему установленного образца, полученных в текущем или предшествующем году – 2 балла;

- 5) наличие аттестата о среднем общем образовании с отличием или аттестата о среднем (полном) общем образовании для награжденных золотой (серебряной) медалью или диплома о среднем профессиональном образовании с отличием, диплома о начальном профессиональном

образовании с отличием или диплома о начальном профессиональном образовании с отличием для награжденных золотой (серебряной) медалью – 10 баллов;

6) осуществление волонтерской (добровольческой) деятельности в течение последних 4 лет – 4 балла;

7) наличие статуса победителя или призера Всероссийской олимпиады или олимпиады школьников (в соответствии с перечнем олимпиад школьников, утверждаемым Минобрнауки России), не используемого для получения особых прав и (или) преимуществ при поступлении на обучение по конкретным условиям поступления и конкретным основаниям приема и полученного не ранее 4 лет до дня завершения приема документов и вступительных испытаний – 10 баллов;

8) наличие статуса победителя мероприятия, включенного в перечень, утвержденный Министерством просвещения Российской Федерации в соответствии с пунктом 4 Правил выявления детей, проявивших выдающиеся способности и сопровождения их дальнейшего развития, полученных не ранее 2 лет до дня завершения приема документов и вступительных испытаний – 10 баллов;

9) наличие статуса победителя (призера) национального и (или) международного чемпионата по профессиональному мастерству среди инвалидов и лиц с ограниченными возможностями здоровья «Абилимпикс» – 10 баллов;

10) наличие статуса победителя Межрегиональной с международным участием многопрофильной олимпиады для школьников "Морской старт" и полученного не ранее 4 лет до дня завершения приема документов и вступительных испытаний – 10 баллов;

11) наличие статуса призера Межрегиональной с международным участием многопрофильной олимпиады для школьников "Морской старт" и полученного не ранее 4 лет до дня завершения приема документов и вступительных испытаний – 8 баллов;

12) наличие статуса участника второго этапа Межрегиональной с международным участием многопрофильной олимпиады для школьников "Морской старт" и полученного не ранее 4 лет до дня завершения приема документов и вступительных испытаний – 4 балла;

13) наличие статуса победителя Открытого городского конкурса-защиты научно-исследовательских работ учащихся, проводимого ГБОУ «Центр дополнительного образования детей «Малая академия наук города Севастополя» и полученного не ранее 4 лет до дня завершения приема документов и вступительных испытаний – 10 баллов;

14) наличие статуса призера Открытого городского конкурса-защиты научно-исследовательских работ учащихся, проводимого ГБОУ «Центр дополнительного образования детей «Малая академия наук города Севастополя» и полученного не ранее 4 лет до дня завершения приема документов и вступительных испытаний – 8 баллов;

15) наличие статуса победителя Всероссийского конкурса «Большая перемена» – 5 баллов;

16) наличие статуса призера Всероссийского конкурса «Большая перемена» – 3 балла;

17) наличие статуса победителя второго (итогового) этапа Всероссийской олимпиады по финансовой грамотности – 10 баллов;

18) наличие статуса призера второго (итогового) этапа Всероссийской олимпиады по финансовой грамотности – 8 баллов;

19) наличие статуса участника второго (итогового) этапа Всероссийской олимпиады по финансовой грамотности – 3 балла;

20) наличие статуса победителя Герценовской олимпиады школьников по иностранным языкам ФГБОУ ВО «Российский государственный педагогический университет им. А.И. Герцена», полученного не ранее 4 лет до дня завершения приема документов и вступительных испытаний – 10 баллов;

21) наличие статуса призера Герценовской олимпиады школьников по иностранным языкам ФГБОУ ВО «Российский государственный педагогический университет им. А.И. Герцена», полученного не ранее 4 лет до дня завершения приема документов и вступительных испытаний – 8 баллов;

22) наличие статуса участника второго этапа Герценовской олимпиады школьников по

иностранным языкам ФГБОУ ВО «Российский государственный педагогический университет им. А.И. Герцена», полученного не ранее 4 лет до дня завершения приема документов и вступительных испытаний – 4 балла;

23) Наличие статуса победителя Межвузовской олимпиады школьников «Первый успех» ФГБОУ ВО «Российский государственный педагогический университет им. А.И. Герцена», полученного не ранее 4 лет до дня завершения приема документов и вступительных испытаний - 10 баллов;

24) Наличие статуса призера Межвузовской олимпиады школьников «Первый успех» ФГБОУ ВО «Российский государственный педагогический университет им. А.И. Герцена», полученного не ранее 4 лет до дня завершения приема документов и вступительных испытаний - 8 баллов;

25) Наличие статуса участника второго этапа Межвузовской олимпиады школьников «Первый успех» ФГБОУ ВО «Российский государственный Правила приема в ФГАОУ ВО СевГУ на обучение по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в 2022 году педагогический университет им. А.И. Герцена», полученного не ранее 4 лет до дня завершения приема документов и вступительных испытаний - 4 балла;

26) наличие статуса победителя второго (итогового) этапа Международной олимпиады по финансовой безопасности – 10 баллов;

27) наличие статуса призера второго (итогового) этапа Международной олимпиады по финансовой безопасности – 8 баллов;

28) наличие статуса участника второго (итогового) этапа Международной олимпиады по финансовой безопасности – 4 балла.

Сумма баллов, начисленных поступающему за индивидуальные достижения, не может быть более 10 баллов.

Баллы, начисленные за индивидуальные достижения, включаются в сумму конкурсных баллов.

2. Характеристика профессиональной деятельности выпускников

2.1. Общее описание профессиональной деятельности выпускников

Области профессиональной деятельности и (или) сферы профессиональной деятельности, в которых выпускники, освоившие программу бакалавриата по направлению подготовки «Информационная безопасность» (далее - выпускники), могут осуществлять профессиональную деятельность (согласно ФГОС):

- образование и наука (в сфере научных исследований);
- связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере);
- обеспечение безопасности (в сфере эксплуатации технических и программно-аппаратных средств защиты информации);
- сфера обороны и безопасности;
- сфера правоохранительной деятельности.

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

Объектами профессиональной деятельности выпускников, освоивших программу бакалавриата, являются:

- объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы,

информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере;

- технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;

- процессы управления информационной безопасностью защищаемых объектов.

Типы задач профессиональной деятельности, к решению которых готовятся выпускники, освоившие программу бакалавриата:

- эксплуатационный;

- проектно-технологический;

- экспериментально-исследовательский;

- организационно-управленческий.

ООП бакалавриата ориентирована на все виды профессиональной деятельности, к которым готовится бакалавр.

Перечень основных объектов (или областей знания) профессиональной деятельности выпускников по направлению подготовки 10.03.01 «Информационная безопасность»:

- объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере;

- технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;

- процессы управления информационной безопасностью защищаемых объектов.

2.2. Перечень профессиональных стандартов, соотнесенных с ФГОС ВО

Основная образовательная программа высшего образования – программа бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (направленность (профиль): Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)) разработана в соответствии с требованиями:

- Профессионального стандарта 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 03.11.2016 № 608н (зарегистрирован Министерством юстиции Российской Федерации 25.11.2016, регистрационный № 44449);

- Профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 01.11.2016 № 598н (зарегистрирован Министерством юстиции Российской Федерации 28.11.2016, регистрационный № 44464);

- Профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15.09.2016 № 522н (зарегистрирован Министерством юстиции Российской Федерации 28.09.2016, регистрационный № 43857);

- Профессионального стандарта 06.034 «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 01.11.2016 № 599н (зарегистрирован Министерством юстиции Российской Федерации 28.09.2016, регистрационный № 44443).

Бакалавр по информационной безопасности должен выполнять обобщенные трудовые функции и трудовые функции, имеющие отношение к профессиональной деятельности, указанные в таблице 2.1.

Таблица 2.1

Область профессиональной деятельности (по Реестру Минтруда)	Обобщенная трудовая функция	Трудовая функция
Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи от несанкционированного доступа к ним (06.030)	Обеспечение защиты от НСД сооружений и СССЭ (за исключением сетей связи специального назначения) в процессе их эксплуатации	Мониторинг функционирования СССЭ, защищенности от НСД сооружений и СССЭ
		Управление функционированием СССЭ, защищенностью от НСД сооружений и СССЭ
		Управление персоналом, обслуживающим сооружения и СССЭ, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от НСД
Защита информации в компьютерных системах и сетях (06.032)	Администрирование средств защиты информации в компьютерных системах и сетях	Администрирование подсистем защиты информации в операционных системах
		Администрирование программно-аппаратных средств защиты информации в компьютерных сетях
		Администрирование средств защиты информации прикладного и системного программного обеспечения
Обеспечение безопасности информации в автоматизированных системах (06.033)	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	Диагностика систем защиты информации автоматизированных систем
		Администрирование систем защиты информации автоматизированных систем
		Управление защитой информации в автоматизированных системах
		Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций
		Мониторинг защищенности информации в автоматизированных системах
		Аудит защищенности информации в

Область профессиональной деятельности (по Реестру Минтруда)	Обобщенная трудовая функция	Трудовая функция
	Внедрение систем защиты информации автоматизированных систем	автоматизированных системах
		Установка и настройка средств защиты информации в автоматизированных системах
		Разработка организационно-распорядительных документов по защите информации в автоматизированных системах
		Анализ уязвимостей внедряемой системы защиты информации
		Внедрение организационных мер по защите информации в автоматизированных системах
Техническая защита информации (06.034)	Проведение работ по установке и техническому обслуживанию защищенных технических средств обработки информации	Проведение работ по установке, настройке и испытаниям защищенных технических средств обработки информации
		Проведение работ по техническому обслуживанию защищенных технических средств обработки информации
	Проведение контроля защищённости информации	Проведение специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации
		Проведение контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок
		Проведение контроля защищенности акустической речевой информации от утечки по техническим каналам
		Проведение контроля защищенности информации от несанкционированного доступа

2.3. Перечень основных задач профессиональной деятельности выпускников

Выпускник, освоивший программу бакалавриата, готов решать профессиональные задачи, указанные в таблице 2.2.

Таблица 2.2.

Область профессиональной деятельности (по Реестру Минтруда)	Типы/виды задач профессиональной деятельности	Задачи профессиональной деятельности
Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи от несанкционированного доступа к ним (06.030) Защита информации в компьютерных системах и сетях (06.032) Обеспечение безопасности информации в автоматизированных системах (06.033) Техническая защита информации (06.034)	Эксплуатационная деятельность	Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований
		Администрирование подсистем информационной безопасности объекта
		Участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем
Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи от несанкционированного доступа к ним (06.030) Защита информации в компьютерных системах и сетях (06.032) Обеспечение безопасности информации в автоматизированных системах (06.033) Техническая защита информации (06.034)	Проектно-технологическая деятельность	Сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности
		Проведение проектных расчетов элементов систем обеспечения информационной безопасности
		Участие в разработке технологической и эксплуатационной документации
		Проведение предварительного технико-экономического обоснования проектных расчетов
Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей	Экспериментально-исследовательская деятельность	Сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования

электросвязи от несанкционированного доступа к ним (06.030) Защита информации в компьютерных системах и сетях (06.032) Обеспечение безопасности информации в автоматизированных системах (06.033) Техническая защита информации (06.034)		Проведение экспериментов по заданной методике, обработка и анализ их результатов
		Проведение вычислительных экспериментов с использованием стандартных программных средств
Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи от несанкционированного доступа к ним (06.030) Защита информации в компьютерных системах и сетях (06.032) Обеспечение безопасности информации в автоматизированных системах (06.033) Техническая защита информации (06.034)	Организационно-управленческая деятельность	Осуществление организационно-правового обеспечения информационной безопасности объекта защиты
		Организация работы малых коллективов исполнителей
		Участие в совершенствовании системы управления информационной безопасностью
		Изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа
		Контроль эффективности реализации политики информационной безопасности объекта защиты

3. Планируемые результаты освоения ООП

Результаты освоения ООП ВО определяются приобретаемыми выпускником компетенциями, т.е. его способностью применять знания, умения и личные качества в соответствии с задачами профессиональной деятельности.

Индикаторы достижения компетенций представлены в таблицах 3.1-3.4.

Таблица 3.1. Универсальные компетенции (УК).

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника	Индикаторы достижения универсальной компетенции
Системное и критическое мышление	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход	УК-1.1: - знает методы и современные средства и технологии поиска информации; - знает методы и способы фильтрации,

	для решения поставленных задач	анализа и оценки достоверности информации; - знает методы анализа и декомпозиции задачи; - знает методы системного подхода к решению задачи; - знает способы и алгоритмы построения логических умозаключений на основе поступающих информации и данных; - знает современные способы, методы и цифровые средства управления (поиска, анализа, синтеза) информацией и данными при решении задач в областях Big Data и Data Mining; - знает способы и методы критического анализа информации и данных в областях Big Data и Data Mining УК-1.2: - умеет анализировать задачу; - умеет применять методы и современные средства поиска информации; - умеет применять методы и способы фильтрации, анализа и оценки достоверности информации; - умеет применять методы анализа и декомпозиции задачи; - умеет применять методы системного подхода к решению задачи; - умеет применять способы и алгоритмы построения логических умозаключений на основе поступающих информации и данных; - умеет применять современные способы, методы и цифровые средства управления (поиска, анализа, синтеза) информацией и данными при решении задач в областях Big Data и Data Mining; - умеет использовать способы и методы критического анализа информации и данных в областях Big Data и Data Mining УК-1.3: - владеет навыками поиска информации с использованием современных средств и технологий; - владеет навыками применения методов и способов фильтрации, анализа и оценки достоверности информации; - владеет методами анализа и декомпозиции задачи; - владеет методами системного подхода к
--	---------------------------------------	---

		решению задачи; - владеет навыками применения способов и алгоритмов построения логических умозаключений на основе поступающих информации и данных; - владеет навыками применения современных способов, методов и цифровых средств управления (поиска, анализа, синтеза) информацией и данными при решении задач в областях Big Data и Data Mining; - владеет навыками применения способов и методов критического анализа информации и данных в областях Big Data и Data Mining
Разработка и реализация проектов	УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1: - знает действующие правовые нормы в области информационной безопасности; - знает стандартные модели, алгоритмы и методы решения стандартных задач анализа инцидентов информационной безопасности; - знает способы и методики, применяемые для генерации новых идей, поиска нестандартных моделей, новых алгоритмов, способов решения задач анализа инцидентов информационной безопасности
		УК-2.2: - умеет формулировать в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение; - умеет проектировать решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений, в том числе с помощью цифровых инструментов; - умеет применять способы и методики, помогающие в генерации новых идей, поиске нестандартных моделей, новых оптимальных алгоритмов, способов решения задач анализа инцидентов информационной безопасности
		УК-2.3: - владеет навыками определения круга задач в рамках поставленной цели и выбора оптимальных способов их

		решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; - владеет навыками генерации новых идей для решения нестандартных задач анализа инцидентов информационной безопасности, цифровой экономики; - владеет навыками абстрагирования от стандартных моделей при решении нестандартных задач анализа инцидентов информационной безопасности, цифровой экономики; - владеет навыками перестроения сложившихся способов решения нестандартных задач анализа инцидентов информационной безопасности, цифровой экономики; - владеет навыками выработки новых оптимальных алгоритмов действий при решении нестандартных задач анализа инцидентов информационной безопасности, цифровой экономики
Командная работа и лидерство	УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3.1: - знает методы реализации своей роли в команде; - знает методы организации межличностного и группового взаимодействия, эффективной коммуникации в команде; - знает методы командообразования, командного взаимодействия на основе знаний менеджмента, психологии, права; - знает методологию достижения успеха с применением современных управленческих методов, информационных технологий и технологий форсайта в командной работе для получения оптимальных результатов реализации проекта; - знает содержание инклюзивного подхода в социальном и профессиональном взаимодействии; - знает современные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей; - знает принципы и способы кооперации с другими людьми для достижения поставленных целей
		УК-3.2:

		- умеет реализовывать свою роль в команде; - умеет организовать межличностное и групповое взаимодействие, эффективную коммуникацию в команде используя методы командообразования, командного взаимодействия на основе знаний менеджмента, психологии, права; - умеет использовать методологию достижения успеха с применением современных управленческих методов, информационных технологий и технологий форсайта в командной работе для получения оптимальных результатов реализации проекта; - умеет реализовывать инклюзивный подход в социальном и профессиональном взаимодействии; - умеет использовать современные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей; - умеет применять на практике принципы и способы кооперации с другими людьми для достижения поставленных целей
		УК-3.3: - владеет навыками реализации своей роли в команде; - владеет навыками организации межличностного и группового взаимодействия, эффективной коммуникации в команде с использованием методов командообразования, командного взаимодействия на основе знаний менеджмента, психологии, права; - владеет навыками применения методологии достижения успеха с применением современных управленческих методов, информационных технологий и технологий форсайта в командной работе для получения оптимальных результатов реализации проекта; - владеет навыками реализации инклюзивного подхода в социальном и профессиональном взаимодействии; - владеет навыками применения современных цифровых средств, позволяющих во взаимодействии с другими людьми достигать поставленных

		целей; - владеет навыками применения принципов и способов кооперации с другими людьми для достижения поставленных целей
Коммуникация	УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	УК-4.1: - знает коммуникативно приемлемые стиль делового общения, вербальные и невербальные средства взаимодействия с партнерами на государственном(-ых) и иностранном(-ых) языках; - знает современные информационно-коммуникационные технологии, необходимые при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках; - знает правила ведения деловой переписки с учетом особенности стилистики официальных и неофициальных писем, социокультурных различий в формате корреспонденции на государственном(-ых) и иностранном(-ых) языках; - знает правила ведения устных деловых разговоры на государственном(-ых) и иностранном(-ых) языках
		УК-4.2: - умеет правильно выбрать коммуникативно приемлемые стиль делового общения, вербальные и невербальные средства взаимодействия с партнерами на государственном(-ых) и иностранном(-ых) языках; - умеет эффективно использовать информационно-коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках; - умеет вести деловую переписку, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном(-ых) и иностранном(-ых) языках; - умеет коммуникативно и культурно приемлемо вести устные деловые разговоры на государственном(-ых) и

		иностранном(-ых) языках УК-4.3: - владеет навыками выбора коммуникативно приемлемых стиля делового общения, вербальных и невербальных средств взаимодействия с партнерами на государственном(-ых) и иностранном(-ых) языках; - владеет навыками использования информационно-коммуникационных технологий при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном(-ых) и иностранном(-ых) языках; - владеет навыками ведения деловой переписки с учетом особенностей стилистики официальных и неофициальных писем, социокультурных различий в формате корреспонденции на государственном(-ых) и иностранном(-ых) языках; - владеет навыками ведения устных деловых разговоров на государственном(-ых) и иностранном(-ых) языках; - владеет навыками перевода профессиональных текстов с иностранного(-ых) на государственный язык
Межкультурное взаимодействие	УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	УК-5.1: - знает методы поиска информации о культурных особенностях и традициях различных социальных групп, необходимой для саморазвития и взаимодействия; - знает основные требования по уважительному отношению к историческому наследию и социокультурным традициям различных социальных групп, опирающемуся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения; - знает способы конструктивного взаимодействия с людьми с учетом их

		социокультурных особенностей в целях успешного выполнения профессиональных задач и усиления социальной интеграции; - знает различные социокультурные тенденции, факты и явления на основе целостного представления об основах мироздания и перспективах его развития, понимает взаимосвязи между разнообразием мировоззрений и ходом развития истории, науки, представлений человека о природе, обществе, познании и самого себя УК-5.2: - умеет находить и использовать необходимую для саморазвития и взаимодействия с другими информацию о культурных особенностях и традициях различных социальных групп; - умеет уважительно относиться к историческому наследию и социокультурным традициям различных социальных групп, опираясь на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения; - умеет выбирать способы конструктивного взаимодействия с людьми с учетом их социокультурных особенностей в целях успешного выполнения профессиональных задач и усиления социальной интеграции; - умеет анализировать различные социокультурные тенденции, факты и явления на основе целостного представления об основах мироздания и перспективах его развития, взаимосвязи между разнообразием мировоззрений и ходом развития истории, науки, представлений человека о природе, обществе, познании и самого себя УК-5.3: - владеет навыками поиска и применения информации о культурных особенностях и традициях различных социальных групп,
--	--	---

		необходимой для саморазвития и взаимодействия с другими людьми; - владеет навыками уважительного отношения к историческому наследию и социокультурным традициям различных социальных групп, опирающегося на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения; - владеет навыками выбора способов конструктивного взаимодействия с людьми с учетом их социокультурных особенностей в целях успешного выполнения профессиональных задач и усиления социальной интеграции; - владеет навыками анализа различных социокультурных тенденций, фактов и явлений на основе целостного представления об основах мироздания и перспективах его развития, выявления взаимосвязей между разнообразием мировоззрений и ходом развития истории, науки, представлений человека о природе, обществе, познании и самого себя
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	УК-6.1: - знает методы формулировки, постановки и достижения личных и профессиональных целей в соответствии с уровнем своих ресурсов, с учетом приоритетов действий для успешного выполнения порученной работы; - знает важность планирования перспективных целей деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда; - знает способы реализации намеченных целей профессиональной деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда; - знает методы критической оценки эффективности использования времени и других ресурсов и возможностей при

		решении поставленных задач и приобретении новых знаний и навыков УК-6.2: - умеет формулировать и ставить личные и профессиональные цели в соответствии с уровнем своих ресурсов, с учетом приоритетов действий для успешного выполнения порученной работы; - умеет оценивать важность планирования перспективных целей деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда; - умеет реализовывать намеченные цели профессиональной деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда; - умеет критически оценивать эффективность использования времени и других ресурсов и возможностей при решении поставленных задач и приобретении новых знаний и навыков УК-6.3: - владеет навыками формулирования и постановки личных и профессиональных целей в соответствии с уровнем своих ресурсов, с учетом приоритетов действий для успешного выполнения порученной работы; - владеет навыками оценки важности планирования перспективных целей деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда; - владеет навыками реализации намеченных целей профессиональной деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда; - владеет навыками критической оценки эффективности использования времени и других ресурсов и возможностей при решении поставленных задач и
--	--	---

		приобретении новых знаний и навыков
	УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1: - знает основы физической культуры; - знает здоровьесберегающие технологии для поддержания должного уровня физической подготовленности с учетом физиологических особенностей организма и условий реализации социальной и профессиональной деятельности; - знает необходимость планирования своего рабочего и свободного времени для оптимального сочетания физической и умственной нагрузки и обеспечения работоспособности в профессиональной деятельности; - знает необходимость соблюдения и пропагандирования нормы здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности УК-7.2: - умеет применять знания основ физической культуры, выбирать здоровьесберегающие технологии для поддержания должного уровня физической подготовленности с учетом физиологических особенностей организма и условий реализации социальной и профессиональной деятельности; - умеет планировать свое рабочее и свободное время для оптимального сочетания физической и умственной нагрузки и обеспечения работоспособности в профессиональной деятельности; - умеет соблюдать и пропагандировать нормы здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности УК-7.3: - владеет методами физической культуры для поддержания должного уровня физической подготовленности с учетом физиологических особенностей организма и условий реализации социальной и профессиональной деятельности; - владеет навыками выбора здоровьесберегающих технологий для поддержания должного уровня физической

		подготовленности с учетом физиологических особенностей организма и условий реализации социальной и профессиональной деятельности; - владеет навыками планирования своего рабочего и свободного времени для оптимального сочетания физической и умственной нагрузки и обеспечения работоспособности в профессиональной деятельности; - владеет навыками соблюдения и пропагандирования норм здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности
Безопасность жизнедеятельности	УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.1: - знает причины возникновения, признаки, условия возникновения, последствия воздействия опасных и вредных факторов в среде обитания, на производстве, в чрезвычайных ситуациях; - знает принципы, методы и средства организации безопасных условий жизнедеятельности, принимает меры по предупреждению возникновения потенциальных опасностей и ликвидации их последствий, создает безопасные условия жизнедеятельности, оказывает первую помощь; - знает методики прогнозирования возникновения и оценки последствий аварийных, опасных и чрезвычайных ситуаций; - знает порядок применения основных средств защиты, поддержания безопасных условий жизнедеятельности
		УК-8.2: - умеет определять причины возникновения, признаки, условия возникновения, последствия воздействия опасных и вредных факторов в среде обитания, на производстве, в чрезвычайных ситуациях; - умеет использовать в повседневной деятельности принципы, методы и средства организации безопасных условий жизнедеятельности, принимает меры по предупреждению возникновения потенциальных опасностей и ликвидации их последствий, создает безопасные условия жизнедеятельности, оказывает

		первую помощь; - умеет применять методики прогнозирования возникновения и оценки последствий аварийных, опасных и чрезвычайных ситуаций; - умеет применять основные средства защиты, поддерживать безопасные условия жизнедеятельности УК-8.3: - владеет навыками установления причин возникновения, признаков, условий возникновения, последствий воздействия опасных и вредных факторов в среде обитания, на производстве, в чрезвычайных ситуациях; - владеет навыками использования принципов, методов и средств организации безопасных условий жизнедеятельности, принятия мер по предупреждению возникновения потенциальных опасностей и ликвидации их последствий, создания безопасных условий жизнедеятельности, оказания первой помощи; - владеет навыками применения методики прогнозирования возникновения и оценки последствий аварийных, опасных и чрезвычайных ситуаций; - владеет навыками применения основных средств защиты, поддержания безопасных условий жизнедеятельности
Экономическая культура, в том числе финансовая грамотность	УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1: - знает принципы недискриминационного взаимодействия, толерантного восприятия человеческого разнообразия, понимания сущности инвалидности; - знает и понимает особые потребности и особенности функционирования лиц с ограниченными возможностями здоровья (инвалидностью); - знает методы выстраивания социального и профессионального взаимодействия с лицами с ограниченными возможностями здоровья (инвалидностью) с учетом особенностей коммуникации и этических норм взаимодействия УК-9.2: - умеет реализовывать социальную и профессиональную деятельность на основе

		принципов недискриминационного взаимодействия, толерантного восприятия человеческого разнообразия, понимания сущности инвалидности; - умеет с пониманием относиться к особым потребностям и особенностям функционирования лиц с ограниченными возможностями здоровья (инвалидностью); - умеет выстраивать социальное и профессиональное взаимодействие с лицами с ограниченными возможностями здоровья (инвалидностью) с учетом особенностей коммуникации и этических норм взаимодействия
		УК-9.3: - владеет навыками построения социальной и профессиональной деятельности на основе принципов недискриминационного взаимодействия, толерантного восприятия человеческого разнообразия, понимания сущности инвалидности; - владеет способностью понимать особые потребности и особенности функционирования лиц с ограниченными возможностями здоровья (инвалидностью); - владеет навыками построения социального и профессионального взаимодействия с лицами с ограниченными возможностями здоровья (инвалидностью) с учетом особенностей коммуникации и этических норм взаимодействия
Гражданская позиция	УК-10. Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1: - знает и понимает базовые принципы функционирования экономики и экономического развития, цели и формы участия государства в экономике; - знает методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей; - знает способы использования финансовых инструментов для управления личными финансами, контроля собственных экономических и финансовых рисков

		УК-10.2: - умеет использовать базовые принципы функционирования экономики и экономического развития, формулировать цели и формы участия государства в экономике; - умеет применять методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей; - умеет использовать финансовые инструменты для управления личными финансами, контроля собственных экономических и финансовых рисков
		УК-10.3: - владеет знаниями о базовых принципах функционирования экономики и экономического развития, целях и формах участия государства в экономике; - владеет методами личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей; - владеет навыками использования финансовых инструментов для управления личными финансами, контроля собственных экономических и финансовых рисков

Таблица 3.2. Общепрофессиональные компетенции (ОПК).

Код и наименование общепрофессиональной компетенции выпускника	Индикаторы достижения общепрофессиональной компетенции
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1. Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах. ОПК-1.2. Способен администрировать средства защиты информации в компьютерных системах и сетях. ОПК-1.3. Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям. ОПК-1.4. Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.
ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том	ОПК-2.1. Понимает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности. ОПК-2.2. Умеет выбирать современные информационные технологии и программные средства, в том числе

числе отечественного производства, для решения задач профессиональной деятельности	отечественного производства, для решения задач профессиональной деятельности. ОПК-2.3. Обладает навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности.
ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Уметь: применять совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Наделен навыками применения совокупности необходимых математических методов для решения задач обеспечения защиты информации.
ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1. Знать: физические законы и модели, необходимые при решении задач в профессиональной деятельности. ОПК-4.2. Уметь: применять необходимые физические законы и модели для решения задач профессиональной деятельности. ОПК-4.3. Владеть: навыками моделирования для решения задач в профессиональной деятельности.
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1. Знает нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации. ОПК-5.2. Понимает определять необходимые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации. ОПК-5.3. Наделен навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации в организации.
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1. Понимает угрозы безопасности информации и возможные пути их реализации, нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. ОПК-6.2. Способен организовать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. ОПК-6.3. Обладает навыками организации защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-7.1. Знает языки программирования и системы разработки программных средств для решения профессиональных задач. ОПК-7.2. Способен выбирать необходимые языки программирования и системы разработки программных средств для решения профессиональных задач. ОПК-7.3. Обладает навыками применения языков программирования и систем разработки программных средств для решения профессиональных задач.
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1. Знает принципы работы с научной литературой, методы поиска научно-технической информации. ОПК-8.2. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов. ОПК-8.3. Обладает навыками решения профессиональных задач с широким использованием актуальной научно-технической литературы.
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1 Понимать корректность криптографической алгоритмов в современных программных комплексах. ОПК-9.2 Способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. ОПК-9.3 Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1 Знает меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты. ОПК-10.2 Способен формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности. ОПК-10.3 Владеет навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.
ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.1. Иметь знания методики проведения экспериментов, методы обработки, оценки погрешности и достоверности результатов экспериментов. ОПК-11.2. Иметь способность выбирать необходимые методы обработки, оценки погрешности и достоверности результатов эксперимента. ОПК-11.3. Владеет навыками проведения экспериментов по заданной методике, обработки, оценки погрешности и достоверности результатов экспериментов.
ОПК-12. Способен проводить	ОПК-12.1. Понимает принципы работы средств обеспечения

подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	защиты информации; основные стандарты информационной безопасности; общие принципы организации информационных систем. ОПК-12.2. Способен готовить исходные данные для проектирования информационных систем. ОПК-12.3. Владеет методами экономического обоснования проектных решений в области информационной безопасности; методами оценки рисков; методами предотвращения угроз конфиденциальности, целостности и доступности информации.
ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	ОПК-13.1 Знает базовые принципы исторической науки; видеть причинно-следственные связи; основные этапы и закономерности исторического развития России; понимать историческое своеобразие нашей страны. ОПК-13.2 Способен оценивать место и роль страны в современном мире, грамотно проводить исторические параллели. ОПК-13.3 Владеет методом анализа исторических закономерностей.

Таблица 3.3. Общепрофессиональные компетенции, соответствующие направленности (профилю) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» программы бакалавриата (ОПК-2.*).

Код и наименование общепрофессиональной компетенции выпускника	Индикаторы достижения общепрофессиональной компетенции
ОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	ОПК-2.1.1.1: - знает принципы построения систем защиты информации; - знает критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем; - знает основные угрозы безопасности информации и модели нарушителя
	ОПК-2.1.2.1: - умеет анализировать угрозы безопасности информации; - умеет оценивать информационные риски; - умеет применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; - умеет анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей
	ОПК-2.1.3.1: - владеет навыками расчета показателей эффективности защиты информации, обрабатываемой в автоматизированных системах; - владеет навыками проведения анализа уязвимости программных и программно-аппаратных средств

	системы защиты информации
ОПК-2.2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	ОПК-2.2.1.1: - знает организационные меры по защите информации; - знает основные методы управления защитой информации
	ОПК-2.2.2.1: - умеет разрабатывать предложения по совершенствованию системы управления защиты информации; - умеет осуществлять планирование и организацию работы персонала с учетом требований по защите информации
	ОПК-2.2.3.1: - владеет навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации
ОПК-2.3. Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ОПК-2.3.1.1: - знает национальные, межгосударственные и международные стандарты в области защиты информации; - знает нормативные правовые акты в области защиты информации
	ОПК-2.3.2.1: - умеет документировать процедуры и результаты контроля функционирования системы защиты информации
	ОПК-2.3.3.1: - владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы
	ОПК-2.3.1.2: - знает принципы работы и правила эксплуатации программно-аппаратных средств защиты информации; - знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем; - знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации
	ОПК-2.3.2.2: - умеет проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям
	ОПК-2.3.3.2: - владеет навыками разработки программ и методик испытаний опытного образца программно-

	технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям
ОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ОПК-2.4.1.1: - знает критерии оценки защищенности объекта информатизации; - знает технические средства контроля эффективности мер защиты информации; - знает методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации
	ОПК-2.4.2.1: - умеет осуществлять контроль обеспечения уровня защищенности объектов информатизации
	ОПК-2.4.3.1: - владеет навыками оценки защищенности объектов информатизации с помощью типовых программных средств

Таблица 3.4. Профессиональные компетенции (ПК-2.*).

Код и наименование профессиональной компетенции выпускника	Индикаторы достижения профессиональной компетенции
ПК-2.1. Способен обеспечивать защиту от несанкционированного доступа объекта информатизации и сетей связи (за исключением сетей связи специального назначения)	ПК-2.1.1: - знает методы контроля функционирования сетей связи, их защищенности от НСД; - знает принципы построения современных сетей связи, математические модели каналов связи, виды модуляции сигналов; - знает функциональное назначение и основные характеристики средств контроля функционирования сетей связи, их защищенности от НСД; - знает организацию и содержание мониторинга функционирования объекта информатизации и средств связи, их защищенности от НСД; - знает возможные источники и технические каналы утечки информации; - знает нормативные правовые акты в области связи и защиты информации.
	ПК-2.1.2: - умеет использовать средства мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств защиты объекта информатизации и сетей связи от НСД; - умеет проводить контроль функционирования средств и сетей связи, их защищенности от НСД;

	- умеет определять технические характеристики средств и сетей связи, их защищенности от НСД; - умеет оценивать помехоустойчивость и эффективность сетей электросвязи при передаче трафика, оптимизировать их параметры; - умеет осуществлять проверки средств и сетей связи, программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты информации от НСД на соответствие заданным требованиям; - умеет проводить документационное обеспечение функционирования СССЭ, их защищенности от НСД. ПК-2.1.3: - владеет навыками применения средств анализа функциональности средств и сетей связи, их защищенности от НСД; - владеет навыками контроля целостности средств и систем связи, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты от НСД; - владеет навыками составления отчетов по результатам проверок, в том числе выявление инцидентов, которые могут привести к сбоям или нарушению функционирования или возникновению угроз безопасности информации.
ПК-2.2. Способен обеспечить управление защитой информации на объектах информатизации	ПК-2.2.1: - знает основные методы управления защитой информации; - знает основные угрозы безопасности информации и модели нарушителя на объектах информатизации; - знает методы защиты информации от "утечки" по техническим каналам; - знает нормативные правовые акты в области защиты информации; - знает национальные, межгосударственные и международные стандарты в области защиты информации; - знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. ПК-2.2.2: - умеет оценивать информационные риски на объектах информатизации; - умеет классифицировать и оценивать угрозы безопасности информации; - умеет определять подлежащие защите информационные ресурсы объектов информатизации; - умеет применять нормативные документы по противодействию технической разведке; - умеет разрабатывать предложения по совершенствованию системы управления защиты информации на объектах информатизации; - умеет конфигурировать параметры систем защиты

	информации на объектах информатизации; - умеет применять технические средства контроля эффективности мер защиты информации. ПК-2.2.3: - владеет навыками анализа воздействия изменений конфигурации автоматизированной системы на ее защищенность; - владеет навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации на объекте информатизации; - владеет навыками оценки последствий от реализации угроз безопасности информации на объекте информатизации; - владеет навыками анализа изменения угроз безопасности информации объекта информатизации, возникающих в ходе его эксплуатации.
ПК-2.3. Способен внедрять системы защиты информации на объектах информатизации	ПК-2.3.1: - знает основные угрозы безопасности информации и модели нарушителя для объектов информатизации; - знает типовые средства, методы и протоколы идентификации, аутентификации и авторизации; - знает основные меры по защите информации на объектах информатизации; - знает нормативные правовые акты в области защиты информации; - знает нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; - знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; - знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации на объектах информатизации; - знает принципы построения средств защиты информации от "утечки" по техническим каналам и способы защиты от нее; - знает способы контроля эффективности защиты информации от "утечки" по техническим каналам; - знает организационные меры по защите информации; - знает методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации; - знает методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности

	информации; - знает методы, способы и средства обеспечения отказоустойчивости автоматизированных информационных систем.
	ПК-2.3.2: - умеет администрировать программные средства систем защиты информации на объектах информатизации; - умеет устранять известные и выявленные уязвимости автоматизированных систем, приводящие к возникновению угроз безопасности информации; - умеет применять нормативные документы по противодействию технической разведке; - умеет применять аналитические и компьютерные модели объектов информатизации, автоматизированных систем и систем защиты информации; - умеет проводить анализ структурных и функциональных схем защищенных автоматизированных систем; - умеет определять параметры настройки программного обеспечения систем защиты информации на объектах информатизации; - умеет классифицировать и оценивать угрозы информационной безопасности; - умеет контролировать эффективность принятых мер по защите информации на объектах информатизации; - умеет разрабатывать предложения по совершенствованию системы управления защитой информации на объекте информатизации; - умеет проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств.
	ПК-2.3.3: - владеет навыками проведения входного контроля качества комплектующих изделий системы защиты информации на объектах информатизации; - владеет навыками осуществления автономной наладки технических и программных средств систем защиты информации на объектах информатизации; - владеет навыками проведения предварительных и приемочных испытаний систем защиты информации на объектах информатизации; - владеет навыками внесения в эксплуатационную документацию изменений, направленных на устранение недостатков, выявленных в процессе испытаний; - владеет навыками определения правил и процедур управления системой защиты информации на объекте информатизации; - владеет навыками определения правил и процедур выявления инцидентов и реагирования на них; - владеет навыками определения правил и процедур

	мониторинга обеспечения уровня защищенности информации автоматизированной системы; - владеет навыками определения правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации; - владеет навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных систем; - владеет навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации объекта информатизации; - владеет навыками проведения экспертизы состояния защищенности информации на объекте информатизации; - владеет навыками уточнения модели угроз безопасности информации на объекте информатизации.
ПК-2.4. Способен формировать требования к защите информации на объектах информатизации	ПК-2.4.1: - знает основные информационные технологии, используемые на объектах информатизации; - знает основные угрозы безопасности информации и модели нарушителя для объектов информатизации; - знает виды информационных воздействий и критерии оценки защищенности информации на объектах информатизации; - знает методы защиты информации от "утечки" по техническим каналам; - знает программно-аппаратные средства обеспечения защиты информации на объектах информатизации; - знает методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; - знает принципы формирования политики информационной безопасности объектов информатизации; - знает нормативные правовые акты в области защиты информации; - знает национальные, межгосударственные и международные стандарты в области защиты информации; - знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - знает организационные меры по защите информации; - знает методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации; - знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; - знает основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях; - знает способы реализации угроз безопасности в автоматизированных системах.

	ПК-2.4.2: - умеет анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами; - умеет выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и объектов информатизации в целом; - умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации объекта информатизации; - умеет организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем объектов информатизации; - умеет использовать рисковую методологию управления защитой информации в автоматизированной системе объекта информатизации; - умеет определять класс защищенности автоматизированных систем и их составных частей. ПК-2.4.3: - владеет навыками анализа характера обрабатываемой информации и определения перечня информации, подлежащей защите; - владеет навыками выявления степени участия персонала в обработке защищаемой информации; - владеет навыками планирования мероприятий по обеспечению защиты информации на объекте информатизации; - владеет навыками определения требуемого класса (уровня) защищенности автоматизированной системы объекта информатизации; - владеет навыками обоснования необходимости использования криптографических средств защиты информации; - владеет навыками разработки отчетных документов и разделов технических заданий.
ПК-2.5. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-2.5.1: - знает алгоритмы выполнения работ по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ПК-2.5.2: - умеет выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

	ПК-2.5.3: - владеет навыками установки, настройки, администрирования, обслуживания и проверки работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
--	--

4. Документы, регламентирующие структуру, содержание и организацию образовательного процесса при реализации ООП

4.1. Учебный план и календарный учебный график

В календарном учебном графике указывается последовательность реализации ООП по годам, включая теоретическое обучение, практики, промежуточные и государственную итоговую аттестации, каникулы. Календарный учебный график разработан в соответствии с требованиями ФГОС ВО и других нормативных правовых документов Российской Федерации, а также локальных нормативных актов Университета. Календарный учебный график представлен в составе учебного плана.

В учебном плане отображается структура ООП ВО – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (направленность (профиль): «Организация и технологии защиты информации» (по отрасли или в сфере профессиональной деятельности)).

Таблица 4.1

Структура ООП		Объем ООП в з.е.
Блок 1	Дисциплины (модули)	216
Блок 2	Практика	18
Блок 3	Государственная итоговая аттестация	6
Объем программы бакалавриата		240

Учебный план включает обязательную часть и часть, формируемую участниками образовательных отношений.

В обязательную часть включены:

- дисциплины (модули) и практики, обеспечивающие формирование общепрофессиональных компетенций, определяемых ФГОС ВО;
- обязательные дисциплины (модули), указанные в пункте 2.2 ФГОС ВО;
- дисциплины (модули) по физической культуре и спорту, реализуемые в рамках Блока 1 «Дисциплины (модули)»;
- дисциплины (модули) и практики, обеспечивающие формирование универсальных компетенций.

В часть, формируемую участниками образовательных отношений, включены:

- дисциплины (модули) и практики, обеспечивающие формирование профессиональных компетенций;
- дисциплины (модули) и практики, обеспечивающие формирование универсальных компетенций.

Объем обязательной части без учета объема государственной итоговой аттестации – 163 зачетных единиц, что составляет 67,9 процента от общего объема программы бакалавриата (согласно ФГОС – не менее 65%).

Учебный план регламентирует перечень и последовательность освоения дисциплин (модулей) и практик, формы и сроки прохождения промежуточной аттестации. В учебном плане указывается общий объем дисциплин (модулей), практик в зачетных единицах, а также объем

контактной и самостоятельной работы обучающихся в часах. Для каждой дисциплины (модуля) в учебном плане указываются виды контактной работы.

Максимальный объем учебной нагрузки обучающегося составляет 54 часа в неделю, включая все виды контактной и самостоятельной работы. В указанный объем не входят факультативные дисциплины и элективные дисциплины по физической культуре и спорту.

Объем контактной работы обучающихся с педагогическими работниками при проведении учебных занятий по программе бакалавриата составляет 50,09 % объема программы бакалавриата, отводимого на реализацию дисциплин (модулей) (согласно ФГОС ВО – не менее 50%).

Максимальный объем контактной работы при освоении ООП по очной форме обучения – 29,7 академического часа в неделю. В указанный объем не входит контактная работа по факультативным дисциплинам и элективным дисциплинам по физической культуре и спорту. Минимальный объем контактной работы для бакалавриата очной формы обучения – 22,7 академического часа в неделю.

Объем факультативных дисциплин составляет 8 зачетных единиц.

Обучающимся обеспечивается возможность освоения дисциплин по выбору, в том числе специализированные условия инвалидам и лицам с ограниченными возможностями здоровья.

Объем каникулярного времени в учебном году определяется настоящей ООП с учетом требований Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденный приказом Минобрнауки России от 6 апреля 2021 г. № 245 и отражается в календарном учебном графике.

4.2. Рабочие программы дисциплин (модулей)

В состав ООП бакалавриата входят рабочие программы всех дисциплин (модулей), перечисленных в утвержденном учебном плане.

Рабочие программы дисциплин содержат следующие разделы:

1. Планируемые результаты обучения по дисциплине, ее объем и место в структуре ООП.
2. Содержание и структура дисциплины.
3. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине.
4. Фонды оценочных средств для проведения текущего контроля успеваемости.
5. Фонды оценочных средств для промежуточной аттестации обучающихся по дисциплине.
6. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины.
7. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины.
8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.
9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Рабочие программы дисциплин (модулей) разработаны кафедрами, обеспечивающими реализацию этих дисциплин (модулей), рассмотрены и утверждены на заседании кафедры «Информационная безопасность».

Аннотации к рабочим программам дисциплин (модулей) представлены в **Приложении А**.

4.3. Программы практик

Практики проводятся в форме практической подготовки.

Практическая подготовка – форма организации образовательной деятельности при освоении образовательной программы в условиях выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на

формирование, закрепление, развитие практических навыков и компетенций по профилю образовательной программы.

В соответствии с ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» Блок 2 «Практика» основной образовательной программы бакалавриата может содержать обязательные, рекомендуемые и дополнительные (устанавливаемые образовательной организацией) типы практик.

В Блок 2 «Практика» в соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность входят учебная и производственная, в том числе преддипломная, практики. Учебная и производственная практики представляют собой вид образовательной деятельности в форме практической подготовки и организуются путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью. Практики закрепляют знания и умения, приобретаемые обучающимися в результате освоения дисциплин, вырабатывают практические навыки и способствуют комплексному формированию универсальных, общепрофессиональных и профессиональных компетенций обучающихся.

В соответствии с утвержденным учебным планом практическая подготовка обучающихся по направлению подготовки 10.03.01 Информационная безопасность (направленность (профиль): Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)) включает следующие типы практик:

- Социальная практика (учебная);
- Ознакомительная практика (учебная);
- Элективные практики (профессиональный трек (FUTURE SKILLS), исследовательский трек, предпринимательский трек) (дополнительный тип производственной практики);
- Преддипломная практика (производственная).

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

Все типы практик являются неотъемлемой частью учебного процесса, его продолжением в условиях работы обучающихся в организациях, деятельность которых соответствует направленности (профилю) программы бакалавриата (далее – профильная организация), или в структурных подразделениях Университета, предназначенных для проведения практической подготовки.

Содержание и планируемые результаты практики определяются соответствующей программой практики настоящей ООП.

4.3.1. Программа учебной практики

Тип учебной практики: Социальная практика. Данный тип учебной практики введен устным распоряжением ректора ФГАОУ ВО «Севастопольский государственный университет». Проводится в 1 и 2 семестрах. Объем - 3 зачетных единицы. Способ проведения Социальной практики: стационарная. Форма проведения практики – дискретно по периодам проведения (распределенная практика), т.е. практика проводится параллельно с основным учебным процессом: в первую половину дня – занятия согласно расписанию, во вторую половину дня – по плану практики.

Структура Социальной практики включает два модуля. Социокультурный модуль реализуется в 1 семестре. Его объем – 1 зачетная единица. Модуль профессионального волонтерства реализуется во 2 семестре. Его объем – 2 зачетных единицы.

Основные цели Социальной практики:

- в ходе социокультурного модуля распределенной учебной (социальной) практики – ознакомление обучающихся с историко-культурным наследием Крыма и Севастополя, с музейными собраниями региона, что позволит им осознать преемственные связи прошлого, настоящего и будущего, будет способствовать самоидентификации личности, познанию себя в социокультурной действительности, научит активно и творчески применять исторические знания в широком спектре социальных взаимодействий, присущих современному миру;

- в ходе модуля профессионального волонтерства распределенной учебной (социальной) практики – формирование у будущих специалистов готовности к осуществлению волонтерской деятельности в профессиональной области (в области обеспечения информационной безопасности).

Основными задачами данного типа учебной практики являются:

а) в ходе социокультурного модуля:

- ознакомление студентов с музейными коллекциями ведущих музеев Севастополя;
- формирование у студентов представлений об основных периодах истории Крыма и Севастополя, нашедших отражение в музейных коллекциях;
- формирование у студентов навыков самостоятельной работы со специальной литературой, умений находить и анализировать необходимую информацию;
- формирование у студентов способности рассматривать события и явления прошлого и современности с позиций значимости историко-культурного наследия, его сохранения, актуализации и трансляции;

б) в ходе модуля профессионального волонтерства:

- знакомство с волонтерским движением;
- освоение направлений и методов волонтерской работы;
- получение опыта работы в области информационной безопасности;
- ознакомление обучающихся со структурой и основными направлениями деятельности профильной организации / структурного подразделения Университета;
- изучение базы практики;
- изучение и определение состава видов информационных технологий, применяемых на базе практики;
- изучение основных средств защиты информационных технологий, применяемых на базе практики (техническое, программное, лингвистическое обеспечение и т.п.);
- описание информационных ресурсов, применяемых на базе практики (базы данных, web-ресурсы, архивы и т.п.);
- формирование у обучающихся комплекса знаний, умений и навыков, необходимых для разработки волонтерских проектов в области обеспечения информационной безопасности;
- привлечение обучающихся к участию в общеуниверситетских мероприятиях различной направленности;
- развитие у обучающихся личностных качеств, необходимых для осуществления волонтерской деятельности в области обеспечения информационной безопасности.

Волонтерство, с точки зрения закона Российской Федерации, подразумевает добровольческую деятельность в форме безвозмездного выполнения общественно-полезных работ, оказания общественно-полезных услуг. Профессиональное волонтерство – деятельность, направленная на получение опыта работы по избранной специальности.

За период прохождения Социальной практики обучающийся должен закрепить теоретические знания, приобретенные при изучении дисциплины «История (история России, всеобщая история)» и модуля «Технологии личностного развития» («Самоменеджмент», «Психологические тренинги»), получить навыки их практического применения в области обеспечения информационной безопасности.

Тип учебной практики: Ознакомительная практика. Проводится в 4 семестре. Объем - 3 зачетных единицы. Способ проведения Ознакомительной практики: стационарная. Форма проведения практики – дискретно по периодам проведения (рассредоточенная практика), т.е. практика проводится параллельно с основным учебным процессом: в первую половину дня – занятия согласно расписанию, во вторую половину дня – по плану практики.

Основная цель Ознакомительной практики: закрепление теоретических знаний, приобретенных при изучении базовых дисциплин, развитие и закрепление практических умений и навыков исследования, анализа и описания защищенных информационных систем.

Основными задачами Ознакомительной практики являются:

- изучение базы практики;
- изучение и определение состава видов информационных технологий, применяемых на базе практике;
- изучение основных средств защиты информационных технологий, применяемых на базе практике (техническое, программное, лингвистическое обеспечение и т.п.);
- описание информационных ресурсов, применяемых на базе практики (базы данных, web-ресурсы, архивы и т.п.);
- получение опыта работы в области информационной безопасности.

За период прохождения Ознакомительной практики обучающийся должен закрепить знания по дисциплинам «Аппаратные средства вычислительной техники обеспечения информационной безопасности», «Физические основы защиты информации», «Защита программ и данных», «Системы распределенных реестров в информационной безопасности», полученные в процессе обучения на 1 и 2 курсах, получить навыки их практического применения.

4.3.2. Программы производственных практик

Тип производственной практики: Элективные практики. Проводится в 6 семестре. Объем – 6 зачетных единиц. Способ проведения Элективных практик: стационарная или выездная. Форма проведения практики – непрерывно.

В соответствии с ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» блок основной образовательной программы бакалавриата «Практика» может содержать обязательные, рекомендуемые и дополнительные (устанавливаемые образовательной организацией) типы практик. Элективные производственные практики – дополнительный тип производственной практики, установленный ФГАОУ ВО «Севастопольский государственный университет».

В рамках Элективных практик у обучающегося имеется возможность продолжить следование выбранной ранее траектории обучения: профессиональный трек (FUTURE SKILLS), исследовательский трек или предпринимательский трек.

Основная (общая) цель Элективных практик: углубление и закрепление знаний и компетенций, полученных в процессе теоретического обучения, изучение опыта создания и применения защищенных информационных технологий и систем для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств или организаций, приобретение студентами практических навыков и опыта профессиональной работы в организации, учреждении, на предприятии.

Основная цель практики профессионального трека (FUTURE SKILLS): углубление и закрепление знаний и навыков, полученных в процессе теоретического обучения и практической подготовки, и приобретение практических навыков и опыта профессиональной работы в организации, учреждении, на предприятии по выбранной компетенции FUTURE SKILLS.

Основная цель практики исследовательского трека: углубление и закрепление знаний и навыков исследовательской деятельности в области обеспечения информационной безопасности, полученных в процессе теоретического обучения и практической подготовки, и приобретение практических навыков и опыта исследовательской деятельности в организации, учреждении, на предприятии.

Основная цель практики предпринимательского трека: углубление и закрепление знаний и навыков предпринимательской деятельности в области обеспечения информационной безопасности, полученных в процессе теоретического обучения и практической подготовки, и приобретение практических навыков и опыта предпринимательской деятельности в организации, учреждении, на предприятии.

Основными (общими) задачами Элективных практик являются:

- закрепление, углубление и развитие знаний, полученных в процессе теоретической подготовки в предшествующий период обучения в соответствии с выбранным треком;
- формирование у обучаемых полного представления о своей профессии;

- выполнение обязанностей на первичных должностях служб защиты информации предприятий, других структурных подразделений, имеющих отношение к информационной безопасности;

- получение практических навыков по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

- получение практических навыков по применению программных средств системного, прикладного и специального назначения, инструментальных средств, языков и систем программирования для решения профессиональных задач;

- получение практических навыков администрирования подсистемы информационной безопасности объекта защиты;

- получение практических навыков по реализации политики информационной безопасности, применению комплексного подхода к обеспечению информационной безопасности объекта защиты;

- получение практических навыков в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

- получение практических навыков в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

- получение практических навыков в выполнении комплекса работ по обеспечению информационной безопасности предприятия;

- изучение организационно-функциональной структуры базы практики;

- расширение представлений о функциональных возможностях защищенных информационных систем;

- усвоение и закрепление навыков самостоятельной работы и самостоятельного решения поставленных задач;

- сбор материала для последующего его использования при изучении учебных дисциплин;

- изучение и определение состава и видов информационных технологий, применяемых на базе практики;

- изучение основных средств защиты информационных технологий, применяемых на базе практики (техническое, программное, лингвистическое обеспечение и т.п.);

- формирование умения анализировать и оценивать свою собственную профессиональную деятельность;

- описание информационных ресурсов, применяемых на базе практики (базы данных, web-ресурсы, архивы и т.п.);

- изучение опыта профессиональной, исследовательской или предпринимательской деятельности на месте прохождения практики;

- получение практических навыков, соответствующих выбранному обучающимся треку.

За период прохождения производственной (элективной) практики обучающийся должен закрепить знания по дисциплинам «Введение в информационную безопасность», «Информационные технологии и программирование», «Основы защиты от внутренних угроз информационной безопасности», «Основы систем обнаружения вторжений», «Физические основы защиты информации», «Методы и средства защиты программного обеспечения», «Документальное обеспечение информационной безопасности», «Системы распределенных реестров в информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации», «Системы защиты баз данных», «Сети и системы передачи информации в информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Криптографические методы защиты информации», «Системы защиты электронного документооборота», «Инженерно-техническая защита информации», полученные в процессе обучения на 1, 2 и 3 курсах, получить навыки их практического применения.

Тип производственной практики: Преддипломная практика. Проводится в 8 семестре. Объем – 6 зачётных единиц. Способ проведения практики: стационарная или выездная. Форма проведения практики – непрерывно.

Основная цель Преддипломной практики: изучение опыта создания и применения защищенных информационных технологий и систем для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств, организаций или корпораций; приобретение навыков практического решения задач защиты информации на рабочем месте; сбор, обработка (анализ) и подготовка материалов для написания выпускной квалификационной работы, выполнение выпускной квалификационной работы.

Основными задачами Преддипломной практики являются:

- углубление знаний, полученных в ходе обучения, развитие навыков их применения в практической области защиты информации;
- расширение представлений о функциональных возможностях защищенных информационных систем;
- усвоение и закрепление навыков самостоятельной работы и самостоятельного решения поставленных задач;
- сбор материала для последующего его использования при написании выпускной квалификационной работы;
- написание выпускной квалификационной работы;
- углубление практических умений и навыков по профессиональной деятельности в рамках направления 10.03.01 Информационная безопасность;
- приобретение практических навыков по сбору и анализу информационных материалов;
- формирование умения анализировать и оценивать свою собственную профессиональную деятельность.

За период прохождения производственной (преддипломной) практики обучающийся должен закрепить знания, полученные в процессе обучения на всех курсах, получить навыки их практического применения, выполнить работы по оформлению выпускной квалификационной работы.

Все типы практик могут проводиться как в профильных организациях г. Севастополя, Республики Крым или Российской Федерации, так и в подразделениях Университета (лабораториях, центрах и др.), обладающих необходимым кадровым и научным потенциалом, а также материально-техническим оснащением. Производственная (элективная) практика должна проводиться в организациях, соответствующих выбранному треку практической подготовки обучающегося.

Общее руководство и контроль над организацией и проведением практики возлагается на кафедру «Информационная безопасность». В случае проведения практики в профильной организации назначается также руководитель практики от профильной организации. Проведение практики в профильных организациях осуществляется на основе договоров с этими организациями. В их число входят: ФГУП «Главный радиочастотный центр», ООО ЦЗИ «Флагман», ООО «Крым Инфо», ООО «Экстрим Безопасность», АО «Удостоверяющий центр», ГКУ «Многофункциональный центр предоставления государственных и муниципальных услуг в городе Севастополе», ГУП С «Севтелеком», Крымское управление Ростехнадзора, ООО «ТРК ЭЛАС», ООО «Севстар ИСПС», ООО «КТК ТЕЛЕКОМ», ГУП РК «Крымэнерго», ООО «Лаборатория кибербезопасности», Центральный банк Российской Федерации, ООО «Международный аэропорт Симферополь», АО «Инфовотч», Управление Федерального казначейства, ФГУП «НПП «Гамма», ЗАО «Интегра-С», ГУ МЧС России, Правительство города Севастополя.

В случае проведения практики в профильной организации, содержание и планируемые результаты практики согласовываются с руководителем практики от профильной организации.

Промежуточная аттестация по итогам практики проводится в форме защиты отчета о прохождении практики. По результатам аттестации выставляется зачет с оценкой (дифференцированный зачет).

4.4. Фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации

Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям ООП (текущий контроль успеваемости и промежуточная аттестация) созданы фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации, которые включают типовые задания, контрольные работы, тесты и иные формы и методы контроля, позволяющие оценить планируемые результаты обучения по каждой дисциплине (модулю); описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания; методические материалы, определяющие процедуры оценивания знаний, умений и навыков.

Фонды оценочных средств для каждой дисциплины (модуля) разработаны кафедрами, обеспечивающими реализацию этой дисциплины (модуля), рассматриваются и утверждаются кафедрой «Информационная безопасность» в составе рабочей программы дисциплины (модуля) основной образовательной программы.

Формами промежуточной аттестации обучающихся являются зачеты, зачеты с оценкой (дифференцированные зачеты), экзамены, которые проводятся в конце каждого семестра, защита курсовой работы, защита отчета о прохождении практики.

4.5. Программа государственной итоговой аттестации

Государственная итоговая аттестация (далее – ГИА), завершающая освоение ООП, является обязательной.

Цель ГИА – определение соответствия результатов освоения обучающимися основной образовательной программы соответствующим требованиям ФГОС ВО.

В ходе проведения ГИА проверяется уровень подготовленности обучающихся к решению профессиональных задач, уровень сформированности у выпускников, освоивших ООП, совокупности компетенций в соответствии с требованиями ФГОС ВО, с учетом профиля реализуемой образовательной программы.

ГИА обучающихся по данной образовательной программе включает подготовку и защиту выпускной квалификационной работы (далее – ВКР).

Программа ГИА включает:

- требования к выпускным квалификационным работам и порядку их выполнения;
- перечень компетенций, уровень сформированности которых оценивается на ГИА.

Порядок подготовки к процедуре защиты и защите ВКР, требования к ВКР определяются локальными нормативными актами Университета, а также методическими указаниями кафедры.

4.6. Фонды оценочных средств государственной итоговой аттестации

Фонды оценочных средств для проведения ГИА включают в себя:

- примерный перечень тем выпускных квалификационных работ;
- описание показателей и критериев оценивания результатов защиты выпускных квалификационных работ, уровня сформированности компетенций;
- описание шкал оценивания;
- методические материалы, определяющие процедуру оценивания результатов освоения образовательной программы.

5. Сведения об условиях реализации ООП

Условия реализации ООП определяются требованиями ФГОС ВО к условиям реализации программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность.

5.1. Общесистемное обеспечение реализации ООП

Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам) и к электронной информационно-образовательной среде Университета. Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают возможность доступа обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), как на территории Университета, так и вне ее.

Электронная информационно-образовательная среда организации обеспечивает:

- доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;
- формирование электронного портфолио обучающегося, в том числе сохранение его работ, рецензий и оценок на эти работы со стороны любых участников образовательного процесса.

В случаях невозможности организации реализации программы бакалавриата в очной форме, допускается реализация программы бакалавриата с применением электронного обучения, дистанционных образовательных технологий. При этом электронная информационно-образовательная среда Организации дополнительно обеспечивает:

- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения программы бакалавриата;
- проведение всех видов учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;
- взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

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

В качестве структурного подразделения, деятельность которого направлена на реализацию образовательных программ высшего образования по специальностям и направлениям подготовки, входящим в укрупненную группу специальностей и направлений подготовки 10.00.00 «Информационная безопасность», приказом исполняющего обязанности ректора ФГАОУ ВО «Севастопольский государственный университет» от 29.12.2017 г. № 1559-п определена кафедра «Информационная безопасность».

5.2. Кадровые условия реализации ООП

Реализация программы бакалавриата обеспечивается педагогическими работниками и научными сотрудниками Университета, а также лицами, привлекаемыми к реализации программы бакалавриата на иных условиях.

Квалификация педагогических работников и научных сотрудников Университета соответствует квалификационным требованиям, указанным в Едином квалификационном справочнике должностей руководителей, специалистов и служащих, разделе "Квалификационные характеристики должностей руководителей и специалистов высшего профессионального и дополнительного профессионального образования", утвержденном приказом Министерства здравоохранения и социального развития Российской Федерации от 11 января 2011 г. № 1н (зарегистрирован Министерством юстиции Российской Федерации 23 марта 2011 г., регистрационный № 20237), и профессиональным стандартам.

Доля педагогических работников Университета, участвующих в реализации программы бакалавриата, и лиц, привлекаемых Университетом к реализации программы бакалавриата на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), ведущих научную, учебно-методическую и (или) практическую работу, соответствующую профилю преподаваемой дисциплины (модуля), составляет 100 процентов (согласно требованиям ФГОС ВО – не менее 70 процентов).

Доля педагогических работников Университета (исходя из количества замещаемых ставок, приведенного к целочисленным значениям) от общего количества лиц, привлекаемых к реализации программы бакалавриата, составляет 83,13 процента (согласно требованиям ФГОС ВО - не менее 55 процентов).

Доля педагогических работников Университета, участвующих в реализации ООП ВО, и лиц, привлекаемых к образовательной деятельности Университета на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), имеющих ученую степень (в том числе ученую степень, полученную в иностранном государстве и признаваемую в Российской Федерации) и (или) ученое звание (в том числе ученое звание, полученное в иностранном государстве и признаваемое в Российской Федерации), составляет 51,88 процента (согласно требованиям ФГОС ВО - не менее 50 процентов).

Доля педагогических работников Университета, участвующих в реализации программы бакалавриата, и лиц, привлекаемых Университетом к реализации программы бакалавриата на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), являющихся руководителями и (или) работниками иных организаций, осуществляющих трудовую деятельность в профессиональной сфере, соответствующей профессиональной деятельности, к которой готовятся выпускники, и имеющих стаж работы в данной профессиональной сфере не менее 3 лет, составляет 16,88 процента (согласно требованиям ФГОС ВО - не менее 3 процентов).

Согласно требованиям ФГОС ВО в реализации программы бакалавриата должен принимать участие минимум один педагогический работник Организации, имеющий ученую степень или ученое звание по научной специальности 05.13.19 "Методы и системы защиты информации, информационная безопасность" или по научной специальности, соответствующей направлениям подготовки кадров высшей квалификации по программам подготовки научно-педагогических кадров в адъюнктуре, входящим в укрупненную группу специальностей и направлений подготовки 10.00.00 "Информационная безопасность".

5.3. Материально-техническое и учебно-методическое обеспечение реализации ООП

Университет обеспечен помещениями, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой бакалавриата, оснащенными оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей), а также помещением для самостоятельной работы обучающихся.

Перечень материально-технического обеспечения, минимально необходимого для реализации программы бакалавриата, включает в себя специально оборудованные помещения для проведения учебных занятий, в том числе лаборатории и специально оборудованные кабинеты (классы, аудитории).

Университет имеет следующие специально оборудованные помещения для проведения учебных занятий:

а) лаборатории:

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

- электротехники, электроники и схемотехники, оснащенные учебно-лабораторными стендами и контрольно-измерительной аппаратурой для измерения частотных свойств, форм и временных характеристик сигналов, средствами для измерения параметров электрических цепей, средствами генерирования сигналов;

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

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

- программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, программно-аппаратными комплексами защиты информации, включающими в том числе криптографические средства защиты информации, средствами контроля и управления доступом в помещения, средствами охранной и пожарной сигнализации;

б) специально оборудованные кабинеты (классы, аудитории):

- информатики, технологий и методов программирования, оснащенные рабочими местами на базе вычислительной техники, подключенные к локальной вычислительной сети и сети "Интернет", сетевым программным обеспечением, обучающим программным обеспечением;

- защищенного документооборота, оснащенный рабочими местами на базе офисной техники, обучающими стендами и материалами;

в) аудиторию (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну;

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

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

Кафедра «Информационная безопасность» имеет лаборатории и специально оборудованные кабинеты (классы, аудитории), обеспечивающие практическую подготовку в соответствии с направленностью (профилем) программы бакалавриата.

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде Университета.

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

Библиотечный фонд Университета укомплектован печатными изданиями из расчета не менее 0,25 экземпляра каждого из изданий, указанных в рабочих программах дисциплин

(модулей), программах практик, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль), проходящих соответствующую практику.

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

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

5.4. Применяемые механизмы оценки качества образовательной деятельности и подготовки обучающихся

Внутренняя оценка качества образовательной деятельности и подготовки обучающихся по образовательной программе (далее – внутренняя оценка качества) проводится Университетом с целью обеспечения выполнения требований действующего законодательства в области высшего образования, исключения возможных рисков и угроз при реализации программы и достижения запланированных показателей (индикаторов).

Функционирование системы внутренней оценки качества в Университете регламентируется локальными нормативными актами Университета.

6. Рабочая программа воспитания

6.1. Цели и задачи воспитания обучающихся при освоении ими образовательной программы.

Цель рабочей программы воспитания – личностное развитие обучающихся и их социализация, проявляющиеся в активной жизнедеятельности обучающихся, их гражданском самоопределении, профессиональном становлении и индивидуально-личностной самореализации в созидательной деятельности.

Задачи:

- воспитание положительного отношения к труду, воспитание социально значимой целеустремленности и ответственности в деловых отношениях;
- обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств, необходимых для эффективной профессиональной деятельности;
- выявление и поддержка талантливой молодежи, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации;
- формирование культуры и этики профессионального общения;
- воспитание внутренней потребности личности в здоровом образе жизни, ответственного отношения к природной и социокультурной среде;
- повышение уровня культуры безопасного поведения;
- развитие личностных качеств и установок, социальных навыков и управленческих способностей.

6.2. Рабочая программа воспитания представлена в Приложении Б.

6.3 Календарный план воспитательной работы представлен в Приложении к Рабочей программе воспитания.

ЛИСТ ИЗМЕНЕНИЙ
основной образовательной программы
по направлению подготовки
10.03.01 Информационная безопасность
профиль: Организация и технологии защиты информации (по отрасли
или в сфере профессиональной деятельности)
2022 год набора

Компонент ООП (раздел, подраздел, пункт компонента ООП)	Основания для изменений	Краткая характеристика вносимых изменений
Общая характеристика ООП (абзац 3 подпункта пункта 1.2. «Нормативные документы для разработки ООП»)	Приказ Министерства науки и высшего образования Российской Федерации от 27.02.2023 № 208 «О внесении изменений в федеральные государственные образовательные стандарты высшего образования» (далее – Приказ Минобрнауки России от 27.02.2023 № 208)	Абзац 3 подпункта 1.2.1 пункта 1.2. Нормативные документы для разработки ООП» изложить в следующей редакции: «- Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.03 Информационная безопасность, утвержденного приказом Минобрнауки России от 17.11.2020 № 1427, с изменениями, внесенными приказом Министерства науки и высшего образования Российской Федерации от 27.02.2023 № 208»
Общая характеристика ООП (раздел 3. Планируемые результаты освоения ООП»)	Приказ Минобрнауки России от 27.02.2023 № 208	Наименование компетенции «УК-10. Способен формировать нетерпимое отношение к коррупционному поведению» заменить наименованием «УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности»
Учебный план ООП (справочник компетенций)	Приказ Минобрнауки России от 27.02.2023 № 208	Наименование компетенции «УК-10. Способен формировать нетерпимое отношение к коррупционному поведению» заменить наименованием «УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности»
Рабочая программа дисциплины «Правоведение», «Противодействие коррупции», в том числе фонды оценочных средств по дисциплине	Приказ Минобрнауки России от 27.02.2023 № 208	- Наименование компетенции «УК-10. Способен формировать нетерпимое отношение к коррупционному поведению» заменить наименованием «УК-10. Способен формировать нетерпимое отношение к проявлениям

		экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности» - Перечень индикаторов компетенций дополнить следующими индикаторами: УК-10.1: - знает и понимает сущность современного экстремизма и терроризма, их идеологию, типологию и крайнюю общественную опасность; - знает современную нормативно-правовую базу противодействия экстремизму и терроризму в Российской Федерации; - знает методы информационного противодействия идеологии экстремизма и терроризма; - знает и поддерживает принципы и идеологию патриотизма; УК-10.2: - умеет выявлять и противостоять влияниям экстремизма и терроризма, их идеологии; - умеет правильно применять современную нормативно-правовую базу Российской Федерации для противодействия экстремизму и терроризму; - умеет применять методы информационного противодействия идеологии экстремизма и терроризма; - умеет поддерживать принципы и идеологию патриотизма в условиях информационного влияния чуждых идеологий; УК-10.3: - владеет знаниями о сущности современного экстремизма и терроризма, их идеологии, типологии и крайней общественной опасности; - владеет методами информационного противодействия идеологии экстремизма и терроризма; - владеет принципами и идеологией патриотизма;». - В фондах оценочных средств по дисциплине предусмотреть дополнительные задания для оценки
--	--	---

		результатов освоения компетенции УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности
Программа государственной итоговой аттестации (раздел 2. «Перечень компетенций, уровень сформированности которых оценивается на государственной итоговой аттестации»)	Приказ Минобрнауки России от 27.02.2023 № 208	Наименование компетенции «УК-10. Способен формировать нетерпимое отношение к коррупционному поведению» заменить наименованием «УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности»
Фонды оценочных средств государственной итоговой аттестации (раздел 3. «Описание показателей и критериев оценивания компетенций, а также шкал оценивания»)	Приказ Минобрнауки России от 27.02.2023 № 208	Наименование компетенции «УК-10. Способен формировать нетерпимое отношение к коррупционному поведению» заменить наименованием «УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности»

Проректор по образовательной деятельности



(подпись)

(дата)

В.Р. Душко

Директор Дирекции развития образовательных программ

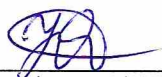


(подпись)

(дата)

У.В. Дремова

Исполняющий обязанности директора
Института информационных технологий



(подпись)

(дата)

Ю.Г. Шаталова

Руководитель образовательной программы
к.т.н., доцент,
заведующий кафедрой

«Информационная безопасность»



(подпись)

(дата)

М.И. Ожиганова

ЛИСТ ИЗМЕНЕНИЙ
основной образовательной программы
по направлению подготовки/специальности
10.03.01 Информационная безопасность
Организация и технологии защиты информации,
год набора 2022 г.

Компонент ООП (раздел, подраздел, пункт компонента ООП)	Основания для изменений	Краткая характеристика вносимых изменений
Общая характеристика ООП	Выписка из протокола №15 заседания ученого совета ФГАОУ ВО «СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» от 26 июня 2025г. п.8.4 Об актуализации учебных планов бакалавриата и специалитета всех направлений подготовки	п. 4.1 «Объем факультативных дисциплин составляет 9 зачетных единиц»
Учебный план		Включить в 7-8 семестры факультативную дисциплину «Молодежь и общество» суммарным объемом 1 з.е (36 ч.).

Проректор по образовательной
деятельности

(подпись)

26.06.2025

(дата)

В.Р. Душко

Директор Дирекции развития
образовательных программ

(подпись)

26.06.2025

(дата)

У.В. Дремова

Директор института

(подпись)

26.06.2025

(дата)

Д.В. Моисеев

Руководитель образовательной программы
ученая степень, ученое звание,
должность

(подпись)

26.06.2025

(дата)

М.И.Ожиганова