Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Куижева Саида Казбековна
Должность: Ректор
Дата подписания: 10.09.2021 18:43:31
Уникальный программный ключ:
71183e1134ef9cfa69b206d48027105c1a975e6f

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Майкопский государственный технологический университет»

УТВЕРЖДАЮ
Ректор _____ С.К. Куижева
«01» апреля 2021 г.

ОСНОВНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ

Уровень высшего образования
Бакалавриат

Направление подготовки
10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
Профиль подготовки
Организация и технология защиты информации

Квалификация (степень)
Бакалавр

Год начала подготовки
2021

Майкоп

СОДЕРЖАНИЕ

1. Общие положения

1.1. Основная образовательная программа высшего образования, реализуемая вузом по направлению подготовки 10.03.01 Информационная безопасность и профилю подготовки «Организация и технология защиты информации».

1.2. Нормативные документы для разработки ОП ВО бакалавриата по направлению подготовки 10.03.01 Информационная безопасность.

1.3. Общая характеристика ОП ВО по направлению подготовки 10.03.01 Информационная безопасность

1.4. Требования к уровню подготовки, необходимому для освоения ОП

2. Характеристика профессиональной деятельности выпускника ОП ВО бакалавриата по направлению подготовки 10.03.01 Информационная безопасность

2.1. Область профессиональной деятельности выпускника.

2.2. Объекты профессиональной деятельности выпускника.

2.3. Виды профессиональной деятельности выпускника.

2.4. Задачи профессиональной деятельности выпускника.

3. Компетенции выпускника ОП ВО бакалавриата, формируемые в результате освоения данной программы.

4. Документы, регламентирующие содержание и организацию образовательного процесса при реализации ОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность

4.1. Календарный учебный график.

4.2. Учебный план подготовки бакалавра.

4.3. Рабочие программы учебных курсов, предметов, дисциплин (модулей).

4.4. Программы практик и организации научно-исследовательской работы обучающихся.

5. Фактическое ресурсное обеспечение ОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность

5.1. Кадровое обеспечение.

5.2. Учебно-методическое и информационное обеспечение.

5.3. Материально-техническое обеспечение.

6. Характеристики среды вуза, обеспечивающие развитие общекультурных и социально-личностных компетенций выпускников

7. Нормативно-методическое обеспечение системы оценки качества освоения обучающимися ОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность

7.1. Фонды оценочных средств для проведения текущего контроля успеваемости, промежуточной и государственной итоговой аттестации.

7.2. Итоговая государственная аттестация выпускников ОП бакалавриата.

8. Материалы, подтверждающие участие работодателей в разработке и реализации ОП.

9. Другие нормативно-методические документы и материалы, обеспечивающие качество подготовки обучающихся.

10. Приложения.

Соответствие профессиональных стандартов по направлению подготовки (специальности) 10.03.01 Информационная безопасность (уровень бакалавриата)

№ п/п	Направление подготовки (специальность)	Профиль подготовки (специализация, магистерская программа)	Соответствующий профессиональный стандарт
1	2	3	4
1	10.03.01 Информационная безопасность (уровень бакалавриата)	10.03.01 Информационная безопасность (Организация и технология защиты информации)	

1. Общие положения

1.1. Введение

Основная образовательная программа бакалавриата, реализуемая в ФГБОУ ВО «МГТУ» по направлению подготовки 10.03.01 Информационная безопасность и профилю подготовки «Организация и технология защиты информации», представляет собой систему документов, разработанную и утвержденную университетом с учетом требований федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01. Информационная безопасность, утвержденного Приказом Министерства науки и высшего образования РФ от 17 ноября 2020 г. N 1427 «Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность».

ОП регламентирует цели, ожидаемые результаты, содержание, условия и технологии реализации образовательного процесса, оценку качества подготовки выпускника по данному направлению подготовки и включает в себя: учебный план, рабочие программы учебных курсов, предметов, дисциплин (модулей) и другие материалы, обеспечивающие качество подготовки обучающихся, а также программы учебной и производственной практики, календарный учебный график и методические материалы, обеспечивающие реализацию соответствующей образовательной технологии.

1.2. Нормативные документы для разработки ОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность

- Нормативную правовую базу разработки ООП бакалавриата составляют:
- - -Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 24.03.2021 г.) «Об образовании в Российской Федерации»;
- - Федеральный государственный образовательный стандарт (ФГОС) по направлению подготовки 10.03.01 Информационная безопасность, утвержденный приказом Министерства образования и науки Российской Федерации от 17.11.2020 № 1427;
- - Приказ Минобрнауки России от 05.04.2017 № 301 «Об утверждении Порядка

организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры» (Зарегистрировано в Минюсте России 14.07.20217г. № 47415;

- - Приказ Минобрнауки России № 885, Минпросвещения России № 390 от 05.08.2020 (ред. от 18.11.2020) «О практической подготовке обучающихся» (вместе с «Положением о практической подготовке обучающихся») (Зарегистрировано в Минюсте России 11.09.2020 № 59778);
- - Федеральный Закон Российской Федерации от 31 июля 2020 г. №304-ФЗ «О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» по вопросам воспитания обучающихся»,
- - Стратегии развития воспитания в Российской Федерации на период до 2025 года, утв. распоряжением Правительства РФ от 29.05.2015 г. №996-р;
- - Приказ Минобрнауки России от 26 ноября 2020 г. N 1456 “О внесении изменений в федеральные государственные образовательные стандарты высшего образования”
- - Нормативно-методические документы Министерства высшего образования и науки России;
- - Устав ФГБОУ ВО «МГТУ»;
- - Нормативно-методические документы ФГБОУ ВО «МГТУ».

Срок освоения ОП бакалавриата: 4 года по очной форме обучения.

Трудоемкость ОП бакалавриата: 240 зачетных единиц, включая все виды аудиторной и самостоятельной работы студента, практики и время, отводимое на контроль качества освоения студентом ОП.

1.3. Требования к уровню подготовки, необходимому для освоения ОП ВО

Для освоения ОП подготовки бакалавра и специалиста абитуриент должен иметь документ государственного образца о среднем (полном) общем образовании или среднем профессиональном образовании.

2. Характеристика профессиональной деятельности выпускника ОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность

2.1. Область профессиональной деятельности и (или) сферы профессиональной деятельности, в которых выпускники, освоившие программу бакалавриата, могут осуществлять профессиональную деятельность:

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

Цель ОПОП ВО - подготовить выпускника – бакалавра, способного обеспечить и организовать защиту информации в автоматизированных (компьютерных, информационных) системах и сетях в условиях существования угроз их информационной безопасности на международном и национальном уровнях, методов их парирования и оценки, со знанием международного и национального информационного права, систем технического регулирования, и нормативной базы.

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

2.2. Объекты профессиональной деятельности выпускника

Объектами профессиональной деятельности выпускников программ бакалавриата с присвоением квалификации «академический бакалавр» 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.

2.3. Виды профессиональной деятельности, к которым готовятся выпускники программ бакалавриата с присвоением квалификации:

- - эксплуатационный
- - организационно-управленческий.

Перечень профессиональных стандартов, соотнесенных с федеральным государственным образовательным стандартом высшего образования по направлению подготовки

№ п/п	Код ПС	Наименование ПС	Реквизиты приказа Министерства труда и социальной защиты Российской Федерации об утверждении ПС
1	06.032	Специалист по безопасности компьютерных систем и сетей	Приказ № 598н от 01.11.2016 г Минтруда России
2	06.033	Специалист по безопасности компьютерных систем и сетей	Приказ № 598н от 01.11.2016 г Минтруда России

2.4. Задачи профессиональной деятельности выпускника

Выпускник программы бакалавриата с присвоением квалификации , в соответствии с видом (видами) профессиональной деятельности, на который (которые) ориентирована программа бакалавриата, готов решать следующие профессиональные задачи:

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, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;

организационно-управленческая деятельность:

- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

- организация работы малых коллективов исполнителей с учетом требований защиты информации;

- участие в совершенствовании системы управления информационной безопасностью;

- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны;

- контроль эффективности реализации политики информационной безопасности объекта.

Требования к результатам освоения ОП, соответствующие ФГОС и учитывающие требования ПС, представлены в виде таблицы (приложение 1).

3. Компетенции выпускника ОП бакалавриата, формируемые в результате освоения данной ОП ВО

Перечень обобщенных трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника основной профессиональной образова-тельной программы высшего образования:

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	код	наименование	уровень квалификации	Наименование	код	уровень (подуровень) квалификации
06.032 Специалист по безопасности компьютерных систем и сетей	B	Администрирование средств защиты информации в компьютерных системах и сетях	6	Администрирование подсистем защиты информации в операционных системах	B/01.6	6
				Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	B/02.6	6
				Администрирование средств защиты информации прикладного и системного программного обеспечения	B/03.6	6
06.033 Специалист по защите информации в автоматизированных системах	B	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	6	Диагностика систем защиты информации автоматизированных систем	B/01.6	6
				Администрирование систем защиты автоматизированных систем	B/02.6	6
				Управление защитой информации автоматизированных систем	B/03.6	6
				Обеспечение работоспособности систем защиты информации при возникновении внештатных ситуаций	B/04.6	6
				Мониторинг защищенности информации в автоматизированных системах	B/05.6	6
				Аудит защищенности информации автоматизированных систем	B/06.6	6
	C	Внедрение систем защиты информации автоматизированных систем	6	Установка и настройка средств защиты информации в автоматизированных системах	C/01.6	6
				Разработка организационно-распорядительных документов по защите информации в автоматизированных системах	C/02.6	6
				Анализ уязвимостей внедряемой системы защиты	C/03.6	6
				Внедрение организационных мер по защите информации в автоматизированных системах	C/04.6	6

В результате освоения программы бакалавриата у выпускника должны

быть сформированы общекультурные, общепрофессиональные, профессиональные компетенции.

В результате освоения данной ОП бакалавриата выпускник должен обладать следующими компетенциями:

Универсальные компетенции выпускника и их индикаторы

Направление категории (группы) универсальных компетенций	**Код и наименование УК выпускника**	**Индикатор УК**	**Дескрипторы индикаторов**	**Соотнесенные дисциплины**
Системное и критическое мышление	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	И.УК.1.1.Способен искать, критически анализировать и осуществлять синтез информации.	Д.УК.1.1.1. Знать принципы поиска, сбора, анализа информации. Д.УК.1.1.2. Уметь осуществлять научный поиск по информационным источникам. Д.УК.1.1.3. Владеть методиками системного подхода для решения поставленных задач.	История (история России, всеобщая история); Философия; Теория информации; Современные информационные технологии; Профайлинг в различных сферах деятельности; Коммуникация на русском и иностранных языках; Современные средства и технологии исследования личности.
		И.УК.1.2.Способен формировать отношение к полученной информации или проблеме, рассматриваемой в ходе решения поставленной задачи.	Д.УК.1.2.1. Уметь систематизировать разнородные данные. Д.УК.1.2.2. Уметь при обработке информации отличать факты от мнений.	
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	И.УК.2.1. Способен проводить анализ поставленной цели.	Д.УК.2.1.1. Знать необходимые для осуществления профессиональной деятельности правовые нормы, нормативно-правовые акты и стандарты в сфере профессиональной деятельности, методологические основы принятия управленческого решения. Д.УК.2.1.2. Владеет методиками анализа поставленной цели.	Основы информационной безопасности; Современные информационные технологии; Технологии обеспечения ИБ; Защищенные ИС; Методы системного анализа систем ИБ; Методы поддержки принятия решений.
		И.УК.2.2. Формулировать задачи, которые необходимо решить для достижения поставленной цели, с учетом нормативно-правовой документации в сфере профессиональной деятельности.	Д.УК.2.2.1. Знать задачи проекта, методы оценки продолжительности и стоимости проекта, а также расчета потребности в ресурсах. Д.УК.2.2.2. Уметь выбирать оптимальные способы достижения поставленной цели.	
Командная работа и лидерство	УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	И.УК.3.1. Способен принимать участие в организации и работе коллектива по выделенному направлению работ.	Д.УК.3.1.1. Знать типологию и факторы формирования команд, способы социального взаимодействия. Д.УК.3.1.2 Уметь действовать в духе сотрудни-	Основы информационной безопасности; Организационное и правовое обеспечение ИБ; Профайлинг в раз-

			чества; принимать решения с соблюдением этических принципов их реализации, проявлять уважение к мнению и культуре других. Д.УК.3.2.1. Владеть навыками распределения ролей в условиях командного взаимодействия. Д.УК3.2.2 Применять методы оценки своих действий, планирование и управление временем.	личных сферах деятельности; Коммуникация на русском и иностранных языках; .Современные средства и технологии исследования личности.
Коммуникация	УК-4 Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке РФ и ин.языке(ах)	И.УК.4.1 Способен применять на практике устные формы коммуникации на русском и иностранном(ых) языке(ах) для решения задач межличностного и профессионального взаимодействия. И.УК.4.2 Способен применять на практике письменные формы коммуникации на иностранном языке для решения задач межличностного и профессионального взаимодействия.	Д.УК.4.1.1 Понимает содержание и импликацию устного выступления (лекция, доклад, ток-шоу и т.п.) по профессиональной тематике, а также спонтанную обращенную речь в рамках профессиональных дискуссий. Д.УК.4.1.2. Выступает с подготовленным докладом по профессиональной тематике на русском и иностранном(ых) языке(ах), логично, структурировано и аргументированно излагая информацию, полученную из различных источников (устных и письменных). Д.УК.4.1.3 Участвует в дискуссиях и иных видах устной профессиональной коммуникации в соответствии с международными нормами общения, а также с прагматическими задачами и установками. Д.УК.4.2.1. Свободно читает и критически оценивает современные тексты (статьи различных жанров, профессиональный блог, посты в социальных сетях, учебную и научную литературу и т.п.) на на русском и иностран-	Иностранный язык (первый); Практический курс первого иностранного языка; Иностранный язык (второй); Практический курс второго иностранного языка; Русский язык и культура речи.

			ном(ых) языке(ах) по профессиональной тематике. Д.УК.4.2.2 Осуществляет переписку на русском и иностранном(ых) языке(ах), связанную с профессиональной деятельностью в соответствии с правилами международного делового общения Д.УК.4.2.3 Логично и структурировано излагает информацию, полученную из различных профессионально-ориентированных источников, в виде отчетов, докладов, рефератов, аналитических эссе.	
Межкультурное взаимодействие	УК-5 Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	И.УК.5.1. Способен интегрировать историю России в контексте мирового исторического развития И.УК.5.2. Отмечать основы и принципы межкультурного взаимодействия в зависимости от социально-исторического, этнического и философского контекста общества	Д.УК.5.1.1. Учитывать при социальном и профессиональном общении историческое наследие и социокультурные традиции различных социальных групп, этносов и конфессий включая мировые религии, философские и этические учения. Д.УК.5.1.2. Владеть принципами недискриминационного взаимодействия при личном и массовом общении в целях выполнения профессиональных задач и усиления социальной интеграции. Д.УК.5.2.1. Анализировать особенности межкультурного взаимодействия (преимущества и возможные проблемные ситуации), обусловленные различием этических, религиозных и ценностных систем. Д.УК.5.2.2. Применять способы межкультурного взаимодействия в различных социокультурных ситуациях, сформировавшихся в ходе исторического раз-	История; Философия; Русский язык и культура речи.

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	И.УК.6.1. Способен реализовывать основные принципы самовоспитания и самообразования, исходя из требований рынка труда. И.УК.6.2. Способен демонстрировать умение самоконтроля и рефлексии, позволяющие самостоятельно корректировать обучение по выбранной профессии.	Д.УК.6.1.1. Уметь использовать новые методы для организации своей работы. Д.УК.6.1.2. Владеть способами управления своей познавательной деятельностью и удовлетворения образовательных интересов и потребностей. Д.УК.6.2.1. Уметь расставлять приоритеты в обучении по избранной профессии. Д.УК.6.2.2. Уметь ставить конкретные цели для профессионального развития и формулировать показатели их достижения	Иностранный язык (первый); Практический курс первого иностранного языка; Практический курс второго иностранного языка; Иностранный язык (второй).
	УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	И.УК.7.1. Роль и значение физической подготовленности для здорового образа жизни и профессиональной деятельности.	Д.УК.7.1.1 Знает виды физических упражнений; научно-практические основы физической культуры и здорового образа и стиля жизни Д.УК.7.1.2. Умеет применять на практике разнообразные средства физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей жизни и профессиональной деятельности; использовать творчески средства и методы физического воспитания для профессионально-личностного развития, физического самосовершенствования, формирования здорового образа и стиля жизни. Д.УК.7.1.3. Владеет средствами и методами укрепления индивидуального здоровья, физического самосовершенствования.	Физическая культура и спорт; Элективные дисциплины по физической культуре и спорту.
Безопасность жизнедеятельности	УК-8 Способен создавать и под-	И.УК.8.1. Способен классифицировать и	Д.УК.8.1.1. Знает принципы, признаки и по-	Безопасность жизнедеятельности

	держивать 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	формулировать принципы организации безопасности труда на предприятии. И.УК.8.2. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности, обеспечить технические средства защиты людей в условиях чрезвычайной ситуации. И.УК.8.3. Формулировать принципы устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	следствия опасностей, способы защиты от чрезвычайных ситуаций. Д.УК.8.1.2. Владеет основами безопасности жизнедеятельности, телефонами служб спасения. Д.УК.8.2.1. Знать условия поддержания безопасных условий жизнедеятельности. Д.УК.8.2.2. Знать правила обеспечения техническими средствами защиты людей в условиях чрезвычайной ситуации. Д.УК.8.3.1. Умеет выявлять признаки, причины и условия возникновения чрезвычайных ситуаций; оценивать вероятность возникновения потенциальной опасности для обучающегося и принимать меры по её предупреждению в условиях образовательного учреждения; оказывать первую помощь в чрезвычайных ситуациях. Д.УК.8.3.2. Владеет методами прогнозирования возникновения опасных или чрезвычайных ситуаций; навыками поддержания безопасных условий жизнедеятельности.	
Экономическая культура, в том числе финансовая грамотность	УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	И.УК.9.1 Базовые принципы функционирования экономики и экономического развития	Д.УК.9.1.1. Владеть основными экономическими понятиями и принципами экономического анализа. Знать основы поведения экономических агентов и принципы рационального выбора. Понимать показатели экономического развития, особенности цикли-	Основы экономики и экономической деятельности в сфере информатизации и информационной безопасности

			ческого развития рыночной экономики, риски инфляции, безработицы, снижение уровня благосостояния в периоды финансово-экономических кризисов, ресурсные ограничения экономического развития Д.УК.9.1.2. Оценивать и анализировать информацию, которая необходима для принятия обоснованных решений в сфере управления личными финансами. Объективно оценивает информацию о перспективах экономического роста и технологического развития экономики страны и отдельной ее отрасли.	
		И.УК.9.2. Цели и формы участия государства в экономике	Д.УК.9.2.1. Понимать цели, задачи, инструменты и эффекты экономической (бюджетной, налоговой, денежно-кредитной, социальной, пенсионной) политики государства и ее влияние на макроэкономические параметры и индивидов. Уметь пользоваться источниками информации о правах и обязанностях потребителя. Уметь пользоваться налоговыми и социальными льготами, формировать личные принципы взаимодействия. 9.2.2. Уметь пользоваться основными расчетными инструментами, правильно выбирать финансовые инструменты для управления личными финансами для достижения поставленных финансовых целей, сравнивать их по критериям доходности, надежности и ликвидности.	

		И.УК.9.3. Экономические и финансовые риски	Д.УК.9.3.1. Владеть понятиями риск и неопределенность, осознавать их неизбежность в экономической и финансовой сфере, знать виды и источники возникновения экономических и финансовых рисков для индивида, способы оценки и их снижения	
		И.УК.9.4. Методы личного экономического роста и финансового планирования	Д.УК.9.4.1. Знать основные этапы жизненного цикла индивида, понимать специфику краткосрочных и долгосрочных финансовых задач на каждом этапе цикла и целесообразность личного экономического и финансового планирования. Знать основные виды личных доходов и расходов, механизмы получения, увеличения, снижения. Д.УК.9.4.2 Решать задачи в сфере личного экономического и финансового планирования, возникающие на всех этапах жизненного цикла. Знать принципы и технологии ведения личного бюджета, уметь вести его, используя существующие программные продукты.	
Гражданская позиция	УК-10 Способен формировать нетерпимое отношение к коррупционному поведению	И.УК.10.1 Анализ правоприменительной практики в сфере противодействия коррупции	Д.УК.10.1.1. Знать нормативные правовые акты в сфере противодействия коррупции Д.УК.10.1.2. Способен выявлять признаки коррупционного поведения. Д.УК.10.1.3. Способен анализировать нормативные правовые и иные акты в сфере противодействия коррупции и практику их применения.	Правоведение; Профайлинг в различных сферах деятельности.
		И.УК.10.2. Профилактическая деятельность в сфере противодействия коррупции	Д.УК.10.2.1. Знать признаки коррупционного поведения Д.УК.10.2.2. Способен применять меры по профилактике коррупции. Д.УК.10.2.3. Способен взаимодействовать в обществе на основе нетерпимого отношения к коррупции.	

Общепрофессиональные компетенции выпускника и их индикаторы

Код и наименование ОПК выпускника	Индикаторы ОПК	Дескрипторы индикаторов	Соотнесенные дисциплины
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	И.ОПК.1.1.Способен понимать стратегию и основные направления развития современного информационного общества.	Д.ОПК.1.1.1. Знать современные информационные технологии. Д.ОПК.1.1.2. Уметь анализировать и оценивать направления развития современного информационного общества	Основы экономики и экономической деятельности в сфере информатизации и информационной безопасности; Основы информационной безопасности; Теория информации; Современные информационные технологии; Организационное и правовое обеспечение информационной безопасности, включая международную информационную безопасность;
	И.ОПК.1.2. Способен понимать направление развития современных информационных технологий и глобальных информационных сетей, информационно-коммуникационные технологии в мировой политике.	Д.ОПК.1.2.1. Владеть навыками аналитической деятельности в области обеспечения информационной безопасности Д.ОПК.1.2.2. Владеть методами анализа и направления развития современных информационных социальных сервисов.	
	И.ОПК.1.3.Способен оценить роль информации и информационной безопасности в современном информационном обществе и цифровой экономике.	Д.ОПК.1.3.1. Иметь навыки поиска информации в глобальной информационной сети Интернет. Д.ОПК.1.3.2. Знать значение информационной безопасности для обеспечения объективных потребностей личности.	
	И.ОПК.1.4.Способен применять методы обеспечения информационной безопасности для обеспечения объективных потребностей личности, общества и государства и оценивать их роль в защите интересов личности, общества и государства.	Д.ОПК.1.4.1. Знать методы обеспечения информационной безопасности личности, общества и государства. Д.ОПК.1.4.2. Владеть навыками оценки роли информации, информационных технологий и информационной безопасности в обеспечении интересов личности, об-	

		щества и государства.	
ОПК-2 - Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	И.ОПК.2.1. Способен использовать на практике знания основ информационной безопасности и защиты данных.	Д.ОПК.2.1.1. Знать аппаратные и программные средства вычислительной техники основные виды и классы операционных систем; сети и сетевые протоколы, основные виды и классы систем управления базами данных, методы коммутации и маршрутизации, данных; сети, сетевые протоколы., современные информационные технологии. Д.ОПК.2.1.2 Знать каналы, в том числе и технические, утечки информации, возможности технических разведок и киберпреступности, виды угроз, уязвимости, способы и средства защиты информации, в том числе и от утечки по техническим каналам, средства криптографической и технической защиты информации; методы и средства контроля эффективности защиты информации и информационных систем.	Основы информационной безопасности; Современные информационные технологии; Электротехника; Электроника и схемотехника; Основы построения и инструменты безопасности операционных систем; Основы построения и инструменты безопасности Баз данных и СУБД; Сети и системы передачи информации; Сетевое и системное администрирование; Основы управления информационной безопасностью; Программно-аппаратные средства защиты информации.
	И.ОПК.2.2. Способен принять участие по выполнению системного анализа комплексного обеспечения информационной безопасности и синтеза системы защиты.	Д.ОПК.2.2.1. Владеть навыками аналитической деятельности в области обеспечения информационной безопасности, основами информационной безопасности. Д.ОПК.2.2.2. Владеть навыками контроля и анализа безопасности баз данных, СУБД, ОС и сетей, современных программно-аппаратных и криптографических средств и системы защиты информации, методы защиты информационных систем.	
	И.ОПК.2.3. Способен принять участие в оценке защищенности созданной системы.	Д.ОПК.2.3.1 Принимать участие в организации и проведении оценки защищенности созданной системы и выполнении ее	

		аудита по требованиям информационной безопасности.	
	И.ОПК.2.4. Способен выполнять работы по установке, настройке, эксплуатации и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты информации.	Д.ОПК.2.4.1. Уметь выбирать необходимые средства защиты информации, формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, средств защиты информации.	
ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности	И.ОПК.3.1. Способен воспроизвести основные понятия и методы теории функций комплексного переменного; основные понятия и методы теории вероятностей и математической статистики; основные понятия и методы математической логики и теории алгоритмов.	Д.ОПК.3.1.1. Знать основные понятия и методы математического анализа, аналитической геометрии, линейной алгебры и теории алгебраических систем. Д.ОПК.3.1.2. Уметь: использовать математические методы и модели для решения прикладных задач. Д.ОПК.3.1.3. Владеть знаниями основных законов физики при решении прикладных задач.	Теория информации; Математика (математический анализ, линейная алгебра и аналитическая геометрия); Физика; Языки программирования; Математическая логика и теория алгоритмов; Теория вероятностей и математическая статистика; Дискретная математика
	И.ОПК.3.2. Способен оценить значение теории информации и кодирования.	Д.ОПК.3.2.1 Владеть навыками математической логики, необходимой для формирования суждений по соответствующим профессиональным проблемам, методами количественного анализа процессов обработки, поиска и передачи информации; навыками проведения физического эксперимента и обработки его результатов Д.ОПК.3.2.2. Уметь применить основные понятия и методы теории вероятностей и математической статистики, математической логики и теории алгоритмов.	
	И.ОПК.3.3. Способен применить инструменты математических методов обработки эксперименталь-	Д.ОПК.3.3.1. Уметь формулировать на математическом языке проблемы,	

	ных данных.	поставленные в терминах других предметных областей; составлять математические модели типовых профессиональных задач и находить способы их решений; интерпретировать профессиональный (физический) смысл полученного математического результата. Д.ОПК.3.3.2 Уметь применять аналитические и численные методы решения поставленных профессиональных задач; приобретать новые математические знания, используя современные образовательные и информационные технологии.	
ОПК-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	И.ОПК.4.1. Способен разбираться в особенностях физических эффектов и явлений, используемых для обеспечения информационной безопасности, относящиеся к профессиональной деятельности с применением методов моделирования, математического анализа, естественнонаучные знания. И.ОПК.4.2. Способен принимать участие в теоретических и экспериментальных исследованиях объектов профессиональной деятельности. И.ОПК.4.3. Способен принимать участие в моделировании физических процессов.	Д.ОПК.4.1.1. Знать основы математики, физики, вычислительной техники и программирования. Д.ОПК.4.1.2. Уметь решать стандартные профессиональные задачи с применением методов математического анализа, моделирования и естественнонаучного знания. Д.ОПК.4.2.1. Владеть основными методами исследований и навыками анализа обеспечения информационной безопасности. Д.ОПК.4.2.2 Владеть навыками проведения физического эксперимента и обработки его результатов. Д.ОПК.4.3.1. Знать принципы работы элементов современной радиоэлектронной аппаратуры, а также физические процессы, протекающие в них. Д.ОПК.4.3.2. Уметь применять основные законы физики при решении задач моделирования при-	Физика; Математика (математический анализ, линейная алгебра и аналитическая геометрия); Математическая логика и теория алгоритмов; Теория вероятностей и математическая статистика; Электротехника; Электроника и схемотехника.

	И.ОПК.4.4. Способен использовать методы количественного анализа процессов обработки, поиска и передачи информации.	кладных процессов. Д.ОПК.4.4.1. Уметь анализировать процессы обработки для решения профессиональных задач. Д.ОПК.4.4.2. Уметь использовать программные и аппаратные средства персонального компьютера; использовать математические методы и модели для решения прикладных задач.	
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	И.ОПК.5.1. Способен участвовать в разработке и формировании комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации, оформлять нормативно-методическую документацию по защите информации в компьютерных системах и сетях с учетом моделей угроз и нарушителей, известных уязвимостей, стандартов, норм информационного права международных и российских нормативно-правовых актов.	Д.ОПК.5.1.1. Знать основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности Российской Федерации; основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; основные российские и международные стандарты зашиты информации, аудита и оценки соответствия требованиям по информационной безопасности, правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы, требования, приказы и стандарты по лицензированию деятельности и сертификации средств	Правоведение; Защита информации от утечки по техническим каналам; Организационное и правовое обеспечение информационной безопасности.

		защиты информации, аттестации автоматизированных (информационных систем); принципы и методы защиты информации, основные положения российской позиции в международных организациях (ООН, ОБСЕ, БРИКС, ШОС и ОДКБ) и в двустороннем формате	
	И.ОПК.5.2. Способен участвовать в проведении анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.	Д.ОПК.5.2.1 Уметь: использовать в практической деятельности правовые знания; анализировать и составлять основные нормативно-правовые акты и осуществлять правовую оценку информации, применительно к профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав; анализировать, толковать и правильно применять правовые нормы, принимать решения и совершать юридические действия в точном соответствии с законом.	
	И.ОПК.5.3. Способен участвовать в подготовке и реализации технико-экономического обоснования	Д.ОПК.5.3.1. Владеть навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками работы с нормативными правовыми актами; профессиональной терминологией.	
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	И.ОПК.6.1 Способен принимать участие в организации работы службы или подразделения информационной безопасности по направлению деятельности.	Д.ОПК.6.1.1 Знать аппаратные средства вычислительной техники; основные операционные системы. Д.ОПК.6.1.2 Владеть информацией о технических каналах утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим	Современные информационные технологии; Организационное и правовое обеспечение информационной безопасности; Защита информации от утечки по техническим каналам; Основы управления информационной безопасностью.

Российской Федерации, Федеральной службы по техническому и экспортному контролю	И.ОПК.6.2. Способен использовать в практической работе знание нормативно-правовых актов, нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	каналам. Д.ОПК.6.1.3 Знать методы и средства контроля эффективности технической защиты информации. Д.ОПК.6.1.4 Владеть принципами противодействия деструктивному или несанкционированному воздействию на информационные вычислительные ресурсы и системы передачи информации. Д.ОПК.6.2.1. Знать нормативно-правовые акты, нормативных и методические документы 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	И.ОПК.7.1. Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач. И.ОПК.7.2. Способность выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах	Д.ОПК.7.1.1. Знать: языки, методы и технологии программирования и методы разработки эффективных алгоритмов решения прикладных задач; основные программные средства системного, прикладного и специального назначения Д.ОПК.7.1.2. Уметь составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные. Д.ОПК.7.2.1. Владеть: навыками применения программных средств системного, прикладного и специального назначения, инструментальных средств, языков и системы программирования для решения профессиональных задач; Д.ОПК.7.2.2. Владеть профессиональной терминологией.	Теория информации; Языки программирования; Технологии и методы программирования; Электроника и схемотехника; Основы управления информационной безопасностью; Программно-аппаратные средства защиты информации; Дискретная математика.
ОПК-8 Способен осуществлять под-	И.ОПК.8.1 Способен осуществлять подбор, изучение и обобще-	Д.ОПК.8.1.1. Знать нормативные документы для	Основы управления информационной

бор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ние научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности. И.ОПК.8.2. Способен применять методы наукометрического поиска международных и российских нормативно-правовых актов, руководящих документов, документов по стандартизации в области и защиты информации	обоснования безопасности информационных систем, отечественные и зарубежные стандарты аудита и оценки защищенности информационных систем, источники информации по проблематике информационной безопасности; Д.ОПК.8.1.2. Уметь собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных отечественных и зарубежных источниках. Д.ОПК.8.2.1. Владеть навыками работы с нормативными правовыми актами; Д.ОПК.8.2.2. Иметь навыки сбора и обработки необходимых данных; навыки анализа и интерпретации информации, содержащейся в различных отечественных и зарубежных источниках, в том числе с использованием электронных журналов и библиотек; профессиональной терминологией.	безопасностью; Организационное и правовое обеспечение информационной безопасности.
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	И.ОПК.9.1 Способен выполнять работы по установке, настройке, эксплуатации и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты информации, проводить контрольные проверки работоспособности применяемых средств защиты информации.	Д.ОПК.9.1.1. Знать аппаратные средства вычислительной техники средства криптографической и технической защиты информации; основные виды и классы операционных систем; сети и сетевые протоколы, основные виды и классы систем управления базами данных, методы коммутации и маршрутизации, данных; сети, сетевые протоколы. Д.ОПК.9.1.2. Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе.	Языки программирования; Организационное и правовое обеспечение информационной безопасности; Электроника и схемотехника; Сети и системы передачи информации; Методы и средства криптографической защиты информации; Дискретная математика.

	И.ОПК.9.2. Способен формулировать и настраивать политики безопасности операционных систем, выбирать режимы работы программно-аппаратных средств криптографической и технической защиты информации в операционных системах настраивать правила фильтрации пакетов в компьютерных сетях	Д.ОПК.9.2.1. Знать основные виды и классы операционных систем; сети и сетевые протоколы, основные виды и классы систем управления базами данных, методы коммутации и маршрутизации, данных. Д.ОПК.9.2.2. Уметь выбирать необходимые средства защиты информации, формулировать и настраивать политику безопасности и средства криптографической и технической защиты информации.	
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	И.ОПК.10.1. Способен участвовать в разработке политики информационной безопасности И.ОПК.10.2. Способен участвовать в формировании комплекса мер по обеспечению информационной безопасности, управлении процес-	Д.ОПК.10.1.1.Знать: аппаратные средства вычислительной техники; основные виды и классы операционных систем; сети и сетевые протоколы, основные виды и классы систем управления базами данных, каналы, в том числе и технические, утечки информации, возможности технических разведок и киберпреступности, виды угроз, уязви-мости, способы и средства защиты информации, в том числе и от утечки по техническим каналам, методы и средства контроля эффективности защиты информации и информационных систем; принципы и методы противодействия деструктивному и несанкционированному воздействию на информационные ресурсы и системы передачи информации; Д.ОПК.10.1.2. Владеть: методикой разработки и формирования политики информационной безопасности. Д.ОПК.10.2.1. Знать организационно-правовую и нормативную базу по организации работы	Основы информационной безопасности; Организационное и правовое обеспечение информационной безопасности; Основы управления информационной безопасностью; Стандартизация информационной безопасности. Национальные и международные системы стандартизации.

	сом их реализации, оформлении нормативно-методической документации по защите информации в компьютерных системах и сетях с учетом моделей угроз и нарушителей, известных уязвимостей международных и российских нормативно-правовых актов. И.ОПК.10.3. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, участвовать в разработке технико-экономического обоснования.	службы информационной безопасности, стандарты, методики и принципы управления коллективом. Д.ОПК.10.2.2. Владеть: навыками организации и обеспечения электронного документооборота, режима конфиденциальности. Д.ОПК10.3.1. Знать организационно-правовую нормативную базу по организации и осуществлению проектирования подсистем информационной безопасности и разработке проектной документации.	
ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов	И.ОПК.11.1. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности. И.ОПК.11.2. Способен принимать участие в проведении экспериментальных исследований систем защиты информации	Д.ОПК.11.1.1. Знать основы теории систем и системного анализа, дискретной математики, теории вероятностей и математической статистики, методов оптимизации и исследования операций, нечётких вычислений, математического и имитационного моделирования Д.ОПК.11.1.2. Понимать основные принципы экспериментальных исследований, соотношение теоретического и экспериментального знания; методы обработки результатов, методы статистического анализа. Д.ОПК.11.2.1. Уметь работать с аппаратурой, приборами и схемами, которые используются в технологических лабораториях, и понимать принципы их действия; ориентироваться в современной и вновь создаваемой технике с целью ее быстрого освоения, внедрения и эффективного использования в практической деятельности,	Теория информации; Языки программирования; Математическая логика и теория алгоритмов; Электротехника; Теория вероятностей и математическая статистика; Организационное и правовое обеспечение информационной безопасности.

		уметь делать оценки и расчеты для анализа явлений и процессов. Д.ОПК.11.2.2. Владеть навыками проведения физического эксперимента и обработки его результатов. Д.ОПК.11.2.3. Владеть навыками чтения электронных схем; профессиональной терминологией; навыками использования технических средств в профессиональной деятельности.	
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	И.ОПК.12.1. Способен участвовать в проведении анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования. И.ОПК.12.2. Способен участвовать в разработке и формировании исходных данных для проектирования средств и систем защиты информации, комплекса мер по	Д.ОПК.12.1.1. Знать: аппаратные средства вычислительной техники; основные виды и классы операционных систем; сети и сетевые протоколы, основные виды и классы систем управления базами данных, каналы, в том числе и технические, утечки информации, возможности технических разведок и киберпреступности, виды угроз, уязвимости, способы и средства защиты информации, в том числе и от утечки по техническим каналам, методы и средства контроля эффективности защиты информации и информационных систем; принципы и методы противодействия несанкционированному и деструктивному воздействию на информационные системы и системы передачи информации. Д.ОПК.12.1.2. Уметь анализировать и оценивать угрозы информационной безопасности объекта и возможные пути их реализации. Д.ОПК.12.2.1. Уметь оформлять нормативно-методическую документацию по защите информации в компьютерных	Современные информационные технологии; Электроника и схемотехника; Основы построения и инструменты безопасности операционных систем; Основы построения и инструменты безопасности Баз данных и СУБД; Сети и системы передачи информации; Сетевое и системное администрирование; Основы управления информационной безопасностью.

	обеспечению информационной безопасности, управлении процессом их реализации.	системах и сетях с учетом моделей угроз и нарушителей, известных уязвимостей международных и российских нормативно-правовых актов. Д.ОПК.12.2.2. Владеть: навыками организации и обеспечения режима конфиденциальности 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.	И.ОПК.13.1 Способен ориентироваться в политических, социальных и экономических процессах. Понимать основные этапы и закономерности исторического развития российского общества, место и роль России в мировой истории и на современном этапе развития. И.ОПК.13.2. Владеть навыками анализа основных этапов и закономерностей исторического развития России, её места и роли в современном мире в целях формирования гражданской позиции и развития патриотизма.	Д.ОПК.13.1.1. Знать: хронологию основных событий истории России, базовые термины и понятия отечественной истории. Д.ОПК.13.1.2. Уметь: ориентироваться в хронологии исторического развития России, использовать базовые знания по отечественной истории в решении профессиональных задач в качестве иллюстраций и аргументов. Д.ОПК.13.2.1. Владеть: начальными навыками анализа отдельных событий отечественной истории в контексте мирового исторического процесса, обобщения исторических данных. Д.ОПК.13.2.2. Уметь использовать базовые знания по всеобщей и отечественной истории для выражения своих мировоззренческих установок и гражданской позиции.	История; Философия.
Компетенции по направленности (профилю) Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности):			
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	И.ОПК.2.1.1. Способен принимать участие в анализе функционального процесса объекта защиты и его информационных составляющих с целью выполнения комплекса мер по обеспечению информационной безопасности, управлять этим процессом.	Д.ОПК.2.1.1.1. Знать аппаратные средства вычислительной техники; основные виды и классы операционных систем; сети и сетевые протоколы, основные виды и классы систем управления базами данных, каналы, в том числе и технические, утечки информации, возможности технических разведок и кибер-	Современные информационные технологии; Основы построения и инструменты безопасности операционных систем; Основы построения и инструменты безопасности Баз данных и СУБД; Сети и системы передачи информации;

ущерба.		преступности, виды угроз, уязвимости, способы и средства защиты информации, в том числе и от утечки по техническим каналам, методы и средства контроля эффективности защиты информации и информационных систем, принципы работы современных информационных систем. Д.ОПК.2.1.1.2 Владеть методическим подходом к анализу функционального процесса объекта защиты и его информационных составляющих, методиками анализа угроз и рисков информационной безопасности, оценки ущерба.	Сетевое и системное администрирование; Основы управления информационной безопасностью.
	И.ОПК.2.1.2. Способен выполнять анализ угроз и обработку рисков информационной безопасности, формулировать модели угроз и нарушителей, политики безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Д.ОПК.2.1.2.1. Знать современные информационные технологии, основы и принципы построения защищенных информационных систем, стандарты и методы, требования по обеспечению информационной безопасности. Д.ОПК.2.1.2.2. Уметь применять комплексный подход к обеспечению информационной безопасности. Д.ОПК.2.1.2.3. Владеть методиками анализа угроз, обработки рисков, формирования моделей угроз и нарушителей.	
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	И.ОПК.2.2.1. Способен принимать участие в формировании и оптимизации инфраструктуры объекта защиты и его системы обеспечения информационной безопасности с целью повышения устойчивости к деструктивным воздействиям, организовывать и поддерживать выполнение комплекса мер по обеспечению устойчивости, управлять процессом их реализации.	Д.ОПК.2.2.1.1 Знать: аппаратные средства вычислительной техники; основные виды и классы операционных систем; сети и сетевые протоколы, основные виды и классы систем управления базами данных, каналы, в том числе и технические, утечки информации, возможности технических разведок и киберпреступности, виды угроз, уязвимости, способы	Организационное и правовое обеспечение информационной безопасности; Основы построения и инструменты безопасности операционных систем; Основы построения и инструменты безопасности Баз данных и СУБД; Сети и системы передачи информации; Сетевое и системное

		и средства защиты информации, в том числе и от утечки по техническим каналам, методы и средства контроля эффективности защиты информации и информационных систем. Д.ОПК.2.2.1.2 Понимать принципы и методы противодействия деструктивному воздействию на информационные ресурсы системы передачи информации.	администрирование; Основы управления информационной безопасностью; Программно-аппаратные средства защиты информации; Организация и управление инцидентами информационной безопасности.
	И.ОПК.2.2.2. Способен разрабатывать и формировать предложения по комплексу мер по обеспечению информационной безопасности с целью повышения устойчивости к деструктивным воздействиям на информационные ресурсы, оформлять нормативно-методическую документацию по защите информации в компьютерных системах и сетях с учетом моделей угроз и нарушителей, известных уязвимостей международных и российских нормативно-правовых актов.	Д.ОПК.2.2.2.1 Анализировать и оценивать угрозы и риски информационной безопасности при деструктивном воздействии на информационные ресурсы системы передачи информации объекта и возможные пути их нейтрализации на этапе оптимизации структуры объекта защиты и структуры системы обеспечения информационной безопасности; Д.ОПК.2.2.2.2. Уметь выполнять работы по установке, настройке, эксплуатации и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты информации, проводить контрольные проверки работоспособности применяемых средств защиты информации.	
	И.ОПК.2.2.3. Способен участвовать в проведении анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, участвовать в проведении технико-экономического обоснования.	Д.ОПК.2.2.3.1. Знать нормативные документы и стандарты по обеспечению информационной безопасности и противодействию к деструктивным воздействиям на информационные ресурсы. Д.ОПК.2.2.3.2. Уметь управлять процессом	

		подготовки и проведения анализа исходных данных для разработки мер противодействия деструктивным воздействиям на информационные ресурсы.	
ОПК-2.3. Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности.	И.ОПК.2.3.1. Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности.	Д.ОПК.2.3.1.1. Знать современные информационные технологии, основы и принципы построения защищенных информационных систем, методы и требования по обеспечению информационной безопасности Д.ОПК.2.3.1.2. Знать правовые основы обеспечения национальной безопасности Российской Федерации; основные нормативные правовые акты в области информационной безопасности и защиты информации, включая документы стратегического планирования, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; основные российские и международные стандарты зашиты информации, аудита и оценки соответствия требованиям по информационной безопасности, правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы, требования, приказы и стандарты по лицензированию деятельности и сертификации средств защиты информации, аттестации автоматизированных (информационных систем); принципы и методы защиты информа-	Организационное и правовое обеспечение безопасности; Основы построения и инструменты безопасности операционных систем; Основы построения и инструменты безопасности Баз данных и СУБД; Сети и системы передачи информации; Сетевое и системное администрирование; Основы управления информационной безопасностью; Стандартизация информационной безопасности. Национальные и международные системы стандартизации.

		ции; Д.ОПК.2.3.1.3. Уметь формулировать постановку задачи по разработке и формированию комплекса мер по обеспечению информационной безопасности.	
	И.ОПК.2.3.2. Может проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, участвовать в разработке технико-экономического обоснования.	Д.ОПК.2.3.2.1. Владеть методиками анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности Д.ОПК.2.3.2.2. Уметь формулировать постановку задачи по разработке и формированию исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, участвовать в проведении технико-экономического обоснования комплекса мер по обеспечению информационной безопасности.	
	И.ОПК.2.3.3. Способен разрабатывать и формировать, комплекс мер по обеспечению информационной безопасности.	Д.ОПК.2.3.3.1 Знать современные информационные технологии, основы и принципы построения защищенных информационных систем Д.ОПК.2.3.3.2. Уметь формировать наборы требований по обеспечению информационной для проектирования подсистем и средств обеспечения информационной безопасности, участвовать.	
	И.ОПК.2.3.4. Может управлять процессом реализации комплекса мер по обеспечению информационной безопасности, оформлять нормативно-методическую документацию по защите информации в компьютерных системах и сетях с учетом моделей угроз и нарушителей, известных уязвимостей международных и российских нормативно-правовых актов	Д.ОПК.2.3.4.1. Знать нормативные документы и стандарты по оформлению конструкторской и эксплуатационной документации Д.ОПК.2.3.4.2. Уметь управлять процессом реализации комплекса мер по обеспечению информационной безопас-	

		ности, оформлять нормативно-методическую и эксплуатационную документацию с учетом моделей угроз и нарушителей, известных уязвимостей международных и российских нормативно-правовых актов.	
ОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	И.ОПК.2.4.1. Способен выполнять роли, предусмотренные методиками аудита, использовать знание современных информационных технологий, основ и принципов построения защищенных информационных систем, методов и требований по обеспечению информационной безопасности, национальных и международных стандартов, нормативно-правовых актов и документов по проведению аудита информационной безопасности.	Д.ОПК.2.4.1.1. Знать современные информационные технологии, основы и принципы построения защищенных информационных систем, методы и требования по обеспечению информационной безопасности 2.4.1.2. Знать организационное и правовое обеспечение информационной безопасности, основы и принципах построения защищенных информационных систем, принципы, правила и методики проведения аудита и оценки соответствия, стандарты и нормативные документы, регламентирующие процесс аудита.	Основы информационной безопасности; Современные информационные технологии; Организационное и правовое обеспечение информационной безопасности; Основы построения и инструменты безопасности операционных систем; Основы построения и инструменты безопасности Баз данных и СУБД; Сети и системы передачи информации; Основы управления информационной безопасностью; Сетевое и системное администрирование; Аудит безопасности информационных систем; Основы управления рисками информационной безопасности.
	И.ОПК.2.4.2. Может принимать участие в организации и проведении аудита информационной безопасности в соответствии с национальными и международными стандартами, нормативно-правовыми актами и документами, регламентирующими проведение аудита информационной безопасности.	Д.ОПК.2.4.2.1 Уметь проводить аудиторскую проверку и организовать работу коллектива аудиторов. Д.ОПК.2.4.2.2. Владеть навыками организации и проведения аудита информационной безопасности по национальным и международным стандартам и нормативным документам.	
	И.ОПК.2.4.3. Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Д.ОПК.2.4.3.1 Уметь проводить работу по организации и проведению аттестации объекта информатизации по требованиям безопасности информации. Д.ОПК.2.4.3.2. Владеть навыками организации и проведения организации и проведению аттестации	

Профессиональные компетенции выпускника и их индикаторы

Код и наименование ПК выпускника	Индикаторы ПК	Дескрипторы индикаторов	Соотнесенные дисциплины
ПК-1 Способен выявлять, классифицировать, оценивать угрозы информационной безопасности, в том числе международной, обрабатывать возникающие риски информационной безопасности, участвовать в работах по разработке и реализации основ политик международной информационной безопасности, в автоматизированных (информационных, компьютерных) системах и сетях.	И.ПК.1.1. Способен выполнять анализ и обработку рисков информационной безопасности, строить модели угроз и нарушителей, применять комплексный подход к обеспечению информационной безопасности объекта защиты И.ПК.1.2 Способен применять принципы построения информационных систем и систем обеспечения информационной безопасности, современных угроз информационной безопасности, методы их анализа и идентификации, требования по информационной безопасности	Д.ПК.1.1.1. Уметь выявлять, анализировать и оценивать угрозы информационной безопасности объекта Д.ПК.1.1.2. Применять методики оценки и обработки рисков информационной безопасности Д.ПК.1.2.1 Знать основы построения операционных систем, СУБД информационных систем и сетей; криптографические стандарты и их использование в информационных системах; способы и средства защиты информации; нормативные документы и стандарты по информационной безопасности Д.ПК.1.2.2. Уметь использовать знание принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации, международные и национальные нормативно-правовые акты, стандарты и нормативно-методические документы по информационной безопасности.	Иностранный язык; Практический курс первого иностранного языка; Практический курс второго иностранного языка; Основы информационной безопасности; Современные информационные технологии; Теория вероятностей и математическая статистика; Организационное и правовое обеспечение информационной безопасности; Основы построения и инструменты безопасности операционных систем; Основы построения и инструменты безопасности Баз данных и СУБД; Сети и системы передачи информации; Сетевое и системное администрирование; Основы управления информационной безопасностью; Программно-аппаратные средства защиты информации;

	И.ПК.1.3 Способен использовать методики анализа угроз и нормативные документы, регламентирующие применение требований стандартов и других документов по информационной безопасности И.ПК.1.4.Способен понимать тенденции и направления развития киберпреступности и угроз информационной безопасности	Д.ПК.1.3.1 Знать методики анализа угроз и рисков информационной безопасности, стандарты и нормативные документы Д.ПК.1.3.2. Выполнять регламенты применения и интерпретации требований стандартов и других документов по информационной безопасности Д.ПК.1.3.3. Владеть методами и средствами парирования угроз безопасности автоматизированным системам; методами технической защиты информации; методами контроля защиты информации Д.ПК.1.4.1. Уметь выявлять, анализировать и оценивать угрозы информационной безопасности объекта Д.ПК.1.4.2. Сравнивать тенденции развития и направления развития киберпреступности в различных странах. Д.ПК.1.4.3. Разрабатывать предложения по противодействию киберпреступности и киберугрозам.	Методы и средства криптографические защиты информации; Аудит безопасности информационных систем; Организация и управление инцидентами ИБ; Основы управления рисками информационной безопасности; Технологии обеспечения информационной безопасности; Защищенные информационные системы; Системы конфиденциального электронного документооборота; Доверенные сервисы безопасности на базе инфраструктуры открытых ключей; Методы системного анализа систем информационной безопасности; Методы поддержки принятия решений; Управление непрерывностью деятельности; Комплексное обеспечение ИБ и основы информационно-аналитической деятельности. Информационная безопасность критических информационных структур; Профайлинг в различных сферах деятельности.
ПК-2 Способен осуществлять поиск, анализ, систематизацию и применение международных нормативно-правовых актов, руководящих документов, документов по стан-	И.ПК.2.1 Способен выполнять анализ событий и проблем в области международной информационной безопасности на основе знания основных международных нормативно-правовых актов, руководящих документов, документов по стандартизации, в области за-	Д.ПК.2.1.1. Знать основы международного и национального информационного права, национальные и международные системы стандартов в области информационной безопасности, а также руководящих документов.	Иностранный язык; Практический курс первого иностранного языка; Практический курс второго иностранного языка; Основы информационной безопасности;

дартизации в области защиты информации и международной информационной безопасности	щиты информации и международной информационной безопасности.	Д.ПК.2.1.2 Владеть методиками поиска, анализа и систематизации международных нормативно-правовых актов, руководящих документов, документов по стандартизации в области защиты информации и международной информационной безопасности	Современные информационные технологии; Организационное и правовое обеспечение информационной безопасности; Основы управления информационной безопасностью; Аудит безопасности информационных систем; Стандартизация информационной безопасности. Национальные и международные системы стандартизации; Основы управления рисками ИБ; Защищенные информационные системы; Системы конфиденциального электронного документооборота.; Доверенные сервисы безопасности на базе инфраструктуры открытых ключей; Комплексное обеспечение ИБ и основы информационно-аналитической деятельности; Информационная безопасность критических информационных структур
	И.ПК.2.2. Способен применять в области международной информационной безопасности и защиты информации методы поиска международных нормативно-правовых актов, руководящих документов, документов по стандартизации	Д.ПК.2.2.1. Знать: основы международного и национального информационного права, национальные и международные системы стандартов в области информационной безопасности, а также руководящих документов, инициативы Российской Федерации по борьбе с киберпреступностью и созданию системы международной информационной безопасности. Д.ПК.2.2.2 Владеть методиками поиска, анализа и систематизации международных нормативно-правовых актов, руководящих документов, документов по стандартизации в области защиты информации и международной информационной безопасности Д.ПК.2.2.3. Учитывать и внедрять руководящие документы по информационной безопасности, разрабатывать нормативно-правовые и организационные меры поддержки работ по обеспечению международной информационной безопасности.	

	И.ПК.2.3 Способен использовать методики анализа угроз и нормативные документы, регламентирующие применение требований стандартов и других документов по информационной безопасности	Д.ПК.2.3.1 Владеть методиками поиска, анализа и угроз, систематизации международных нормативно-правовых актов, руководящих доку-ментов, документами по стандартизации в области защиты информации и международной информационной безопасности Д.ПК.2.3.2 Применять методики анализа угроз и нормативные документы, регламентирующие применение требований стандартов и других документов по информационной безопасности, методики оценки и обработки рисков информационной безопасности	
	И.ПК.2.4 Понимает тенденции и направления развития международной информационной безопасности, законодательства в этой сфере.	Д.ПК.2.4.1. Уметь выявлять, анализировать и оценивать угрозы информационной безопасности объекта Д.ПК.2.4.2. Сравнивать тенденции развития и направления развития киберпреступности в различных странах.	
ПК-3 Способен разрабатывать и применять методики осуществления аналитической деятельности в средствах социальной коммуникации в ходе организации и решения задач информационного противоборства	И.ПК.3.1. Способен выполнять анализ и обработку рисков информационной безопасности в средствах социальной коммуникации в ходе организации и решения задач информационного противоборства.	Д.ПК.3.1.1. Знать принципы работы, способы построения и методы управления средствами социальной коммуникации Д.ПК.3.1.2. Уметь применить методику анализа и обработки рисков информационной безопасности применительно к задачам управления средствами социальной коммуникации и информационного противоборства. Д.ПК.3.1.3. Понимать тенденции и направления развития средств социальной коммуникации.	Основы информационной безопасности; Теория информации; Современные информационные технологии; Организационное и правовое обеспечение ИБ; Сети и системы передачи информации; Сетевое и системное администрирование; Основы управления информационной безопасностью; Аудит безопасности информационных систем; Организация и управление инцидентами ИБ; Культура ИБ; Технологии обеспечения ИБ; Современные информационные социальные
	И.ПК.3.2. Способен принимать участие в построении моделей угроз и нарушителей	Д.ПК.3.2.1. Знать методику построения моделей угроз и нарушителей. Д.ПК.3.2.2. Участвовать в работах по построению моделей угроз и нарушителей.	

			сервисы; Технологии больших данных и основы информационного противоборства; Риски информационной безопасности, философия и основы искусственного интеллекта; Комплексное обеспечение информационной безопасности и основы информационно-аналитической деятельности; Информационная безопасность критических информационных структур; Профайлинг в различных сферах деятельности; Коммуникация на русском и иностранных языках; Современные средства и технологии исследования личности.

Соотнесение обобщенных трудовых функций и трудовых функций работника, входя-щих в профессиональный стандарт с компетенциями выпускника основной профессио-нальной образовательной программы высшего образования

Наименование ПК	Сопряженный ПС	Выбранная ОТФ	ТФ, на подготовку выполнения которых направлена ПК	Конкретные ТД, на подготовку к выполнению которых направлена ПК
ПК-1 Способен выявлять, классифицировать, оценивать угрозы информационной безопасности, в том числе международной, обрабатывать возникающие риски информационной безопасности, участвовать в работах по разработке и реализации основ политик международной информационной безопасности, в	06.032	B6	B/01.6	Разработка порядка применения программно-аппаратных средств защиты информации в операционных системах Контроль корректности функционирования программно-аппаратных средств защиты информации в операционных системах. Обнаружение инцидентов в процессе эксплуатации автоматизированной системы Идентификация инцидентов в процессе эксплуатации автоматизированной системы Оценка защищенности автоматизированных систем с помощью типовых программных средств
	06.033	B6	B/01.6	

автоматизированных (информационных, компьютерных) системах и сетях.				Устранение инцидентов, возникших в процессе эксплуатации автоматизированной системы Расчет показателей эффективности защиты информации, обрабатываемой в автоматизированных системах Инструментальный контроль показателей эффективности защиты информации, обрабатываемой в автоматизированных системах
ПК-2 Способен осуществлять поиск, анализ, систематизацию и применение международных нормативно-правовых актов, руководящих документов, документов по стандартизации в области защиты информации и международной информационной безопасности	06.032 06.033 06.033 06.033 06.033	B6 B6 B6 C6 C6	B/03.6 B/05.6 B/06.06 C/02.6 C/03.6	Определение порядка установки программного обеспечения с целью соблюдения требований по защите информации. Выработка рекомендаций для принятия решений о модернизации системы защиты информации автоматизированной системы. Выявление угроз безопасности информации в автоматизированных системах. Анализ недостатков в функционировании системы защиты информации автоматизированной системы. Оценка информационных рисков. Обоснование критериев эффективности функционирования защищенных автоматизированных систем. Определение правил и процедур управления системой защиты информации автоматизированной системы Определение правил и процедур выявления инцидентов Определение правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы Уточнение модели угроз безопасности информации автоматизированной системы. Проведение анализа уязвимостей автоматизированных и информационных систем.
ПК-3 Способен разрабатывать и применять методики осуществления аналитической деятельности в средствах социальной	06.033	C6	C/02.6	Определение правил и процедур выявления инцидентов. Определение правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы Выбор и обоснование критериев эффективности

коммуникации в ходе организации и решения задач информационного противоборства	06.033	С6	С/03.6	функционирования защищенных автоматизированных систем. Уточнение модели угроз безопасности информации автоматизированной системы. Проведение анализа уязвимостей автоматизированных и информационных систем.
	06.033	С6	С/04.6	Подготовка документов, определяющих правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и возникновению угроз безопасности информации.

4. Документы, регламентирующие содержание и организацию образовательного процесса при реализации ОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность

Содержание и организация образовательного процесса по направлению подготовки 10.03.01 Информационная безопасность регламентируется ФГОС ВО, учебным планом бакалавра с учетом его профиля; рабочими программами учебных курсов, предметов, дисциплин (модулей); материалами, обеспечивающими качество подготовки и воспитания обучающихся; программами учебной, производственной и преддипломной практик; годовым календарным учебным графиком, а также методическими материалами, обеспечивающими реализацию соответствующих образовательных технологий.

4.1. Календарный учебный график

В календарном учебном графике указывается последовательность реализации ОП ВО по годам, включая теоретическое обучения, практики, промежуточные и итоговую аттестацию, каникулы. Календарный график разрабатывается в соответствии с установленными требованиями ФГОС ВО (Приложение 2).

4.2. Учебный план подготовки бакалавра по направлению подготовки 10.03.01 Информационная безопасность (профиль подготовки «Организация и технология защиты информации»).

В учебном плане по направлению подготовки (специальности)

отображается логическая последовательность освоения блоков дисциплин (модулей, практик), обеспечивающих формирование компетенций. Указывается общая трудоемкость дисциплин, модулей, практик в зачетных единицах, а также их общая и аудиторная трудоемкость в часах.

При составлении учебного плана необходимо руководствоваться требованиями к структуре образовательных программ, сформулированными в разделе 6 ФГОС ВО по соответствующему направлению подготовки (специальности).

Для каждой дисциплины (модуля), практики в учебном плане указаны виды учебной работы и формы промежуточной аттестации.

4.3. Рабочие программы учебных курсов, предметов, дисциплин (модулей).

Данная ОП ВО содержит рабочие программы всех учебных курсов, предметов, дисциплин (модулей) как базовой, так и вариативной частей учебного плана, включая дисциплины по выбору студента и факультативные дисциплины. В рабочих программах дисциплин формулируются конечные результаты обучения в органичной увязке с осваиваемыми знаниями, умениями и приобретаемыми компетенциями в целом по ОП с учетом профиля подготовки. Умения и знания, являющиеся основой формирования (совершенствования) компетенций, определяются на основе примерных программ, а также с учетом квалификационных требований, сформулированных в ПС применительно к отдельным трудовым функциям.

Структура и содержание рабочей программы дисциплины (модуля, практики) отражается в локальных нормативных актах (Методические рекомендации по разработке учебно-методического комплекса дисциплины по ФГОС ВО).

4.4. Программы учебной, производственной и преддипломной практик

В соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность по профилю подготовки «Организация и технология защиты информации» раздел основной образовательной

программы бакалавриата «Учебная, производственные и преддипломная практики» является обязательным и представляет собой вид учебных занятий, непосредственно ориентированных на профессионально- практическую подготовку обучающихся. Практики закрепляют знания и умения, приобретаемые обучающимися в результате освоения теоретических курсов, вырабатывают практические навыки и способствуют комплексному формированию общекультурных и профессиональных компетенций обучающихся.

На предприятиях – базах производственных и преддипломной практик общее руководство практикой студентов возлагается приказом руководителя предприятия на одного из руководящих работников или высококвалифицированных специалистов, что позволяет более эффективно и качественно организовать практику.

Все виды практик проводятся на основе договоров, заключенных между университетом и предприятиями, организациями и учреждениями. Базами практик являются ведущие предприятия, учреждения и организации региона, с которыми заключены долгосрочные договора.

Программа учебной практики

При реализации данной ОП предусматривается учебная практика, которая осуществляет знакомство и изучение функций, роли и места защиты информации на предприятии, в организации, учреждении, являющемся базой практики – 2 недели (1 курс, 2 семестр).

Программа производственной практики

1) При реализации данной ОП предусматривается две производственных практики, которые проходят на предприятиях, в организациях, учреждениях, являющихся базами практики - 2 недели (2 курс, 4 семестр), 4 недели (3 курс, 6 семестр).

Цель производственной практики – овладение методами внедрения и эксплуатации систем информационной безопасности, изучение средств и методов защиты информации, приобретение навыков исследования.

Программа преддипломной практики

Преддипломная проводится для выполнения выпускной квалификационной работы и является обязательной – 4 недели (4 курс, 8 семестр).

5. Фактическое ресурсное обеспечение ОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность по профилю подготовки «Организация и технология защиты информации» в ФГБОУ ВО «МГТУ»

Ресурсное обеспечение ОП вуза формируется на основе требований к условиям реализации образовательных программ, определяемых ФГОС ВО по направлению подготовки (специальности), действующей нормативной правовой базой, с учетом рекомендаций примерных ОП и особенностей, связанных с уровнем и профилем образовательной программы.

Ресурсное обеспечение ОП вуза определяется как в целом по ОП, так и по циклам дисциплин и/или модулей, включая в себя:

- кадровое обеспечение;
- учебно-методическое и информационное обеспечение (в т.ч. УМК);
- материально-техническое обеспечение.

5.1. Кадровое обеспечение ОП

Подготовка бакалавров по направлению подготовки 10.03.01 Информационная безопасность по профилю подготовки «Организация и технология защиты информации» осуществляется на факультете информационных систем в экономике и юриспруденции. Выпускающей кафедрой является кафедра информационной безопасности и прикладной информатики. Контингент преподавателей сформирован из специалистов, имеющих базовое образование, соответствующее профилю преподаваемой дисциплины, и систематически занимающихся научной и научно-методической деятельностью.

Общее количество преподавателей, имеющих ученые степени и ученые звания, составляет 80%, в том числе 25%докторов наук, профессоров, кандидатов наук, доцентов 55%; на штатной основе привлекаются 83%.

Организация управления на факультете соответствует уставным

требованиям. Организационно-распорядительная и собственная нормативная документация факультета и кафедр (планы работы, протоколы заседаний кафедр, рабочие учебные планы, учебно-методические комплексы, индивидуальные планы работы преподавателей и т.д.) соответствует действующему законодательству и Уставу университета.

5.2. Учебно-методическое и информационное обеспечение

При подготовке бакалавров уделяется большое внимание обеспечению учебного процесса источниками учебной информации. Преподавание дисциплин осуществляется по учебникам, учебным пособиям, изданным централизованно, а также с использованием методических разработок, конспектов лекций, учебных пособий, написанных преподавателями кафедр.

Образовательная программа по направлению подготовки 10.03.01 Информационная безопасность обеспечена необходимой учебной и научно-технической литературой в соответствии с требованиями государственного образовательного стандарта по всем циклам и разделам изучаемых дисциплин из фонда библиотеки университета.

При разработке ОП должны быть определены учебно-методические и информационные ресурсы (включая учебно-методические комплексы дисциплин и/или модулей), необходимые для реализации данной ОП.

Должен быть обеспечен доступ каждого обучающегося к современным информационным базам данных в соответствии с профилем подготовки. Для обучающихся на старших курсах должна быть обеспечена возможность оперативного получения и обмена информацией с отечественными и зарубежными вузами, предприятиями и организациями.

Каждый обучающийся должен обеспечивается основной учебной и учебно-методической литературой, методическими пособиями, необходимыми для организации образовательного процесса по всем дисциплинам (модулям) ОП в соответствии с нормативами, установленными ФГОС.

Объем фонда основной и дополнительной учебной литературы, имеющей грифы различного уровня, соответствует Минимальным

нормативам обеспеченности вузов учебной базой в части, касающейся библиотечно-информационных ресурсов (Приложение к приказу Минобразования России от 11.04.2001 № 1623).

Фонд дополнительной литературы, помимо учебной, должен включать официальные справочно-библиографические и периодические издания. Фонд периодики должен быть представлен отраслевыми изданиями, соответствующими профилю подготовки, и в обязательном порядке комплектоваться массовыми центральными и местными общественно-политическими изданиями.

Фонд научной литературы должен быть представлен монографиями и периодическими научными изданиями по профилю каждой образовательной программы в соответствии с требованиями, определенными в Приложении к приказу Минобразования России от 11.04.2001 № 1623. Библиотечный фонд должен содержать число наименований отечественных и зарубежных журналов не ниже предусмотренного ФГОС по данному направлению подготовки (специальности).

5.3. Материально-техническое обеспечение

Материально-техническое обеспечение учебного процесса по направлению подготовки 10.03.01 Информационная безопасность полностью соответствует требованиям ФГОС. Кафедры, ведущие подготовку по ОП, оснащены необходимым лабораторным оборудованием и оргтехникой в объеме, достаточном для обеспечения уровня подготовки в соответствии с ФГОС. Компьютеризация обеспечивается компьютерными классами, объединенными в локальную сеть и оснащенными обучающимися и информационными программами, имеется выход в Интернет.

Помещения, предназначенные для изучения профессиональных дисциплин, оснащены современным оборудованием и техническими средствами. Каждый обучающийся имеет возможность доступа к современным информационным базам в соответствии с профилем подготовки кадров, оперативного получения информации и обмена ею.

Выпускающая кафедра располагает достаточным аудиторным фондом

для проведения лекционных, практических и индивидуальных занятий преподавателей со студентами, проведения консультаций и экзаменов, организации и проведения самостоятельной работы студентов, научно-исследовательской работы, дипломного проектирования.

6.Характеристики среды вуза, обеспечивающие развитие общекультурных и социально-личностных компетенций выпускников

Учебно-воспитательная работа на кафедре информационной безопасности и прикладной информатики организована в соответствии с нормативно-правовыми актами федерального, регионального и университетского уровня: Федеральными законами «Об образовании», «О высшем и послевузовском образовании», Концепцией воспитательной работы университета, Уставом университета, планами воспитательной работы университета, факультета и кафедры.

Планирование воспитательной работы кафедра осуществляет и конкретизируется с учетом плана работы университета, на основе рекомендаций, разработанных отделом воспитательной работы для структурных подразделений. Планы работы факультета и кафедры согласовывают между собой структурно и содержательно.

Учебно-воспитательная работа кафедры информационной безопасности и прикладной информатики предусматривает четкую организацию и управление учебным процессом, поскольку студента воспитывает и отношение преподавателя к работе, его объективность, справедливость, принципиальность, дисциплинированность. Целевой установкой концепции воспитательной работы является социализация личности гражданина России, формирование его умения познавать мир и умело строить рационально организованное общество. При этом принята следующая структура этой цели: утверждение общечеловеческих и нравственных ценностей; расширение мировоззрения будущих специалистов; развитие творческого мышления; приобщение к богатству национальной и мировой истории и культуры; овладение коммуникативными основами; обеспечение образовательного и этического уровня; активное воспитание у студентов личных, гражданских и

профессиональных качеств, отвечающих интересам развития личности, общества, создание истинно гуманитарной среды обитания.

Действующая система воспитательной работы в ФГБОУ ВО «МГТУ» предполагает три интегрированных направления, а именно профессионально-трудовое, гражданско-правовое, культурно-эстетическое и нравственное воспитание. Вся воспитательная политика предусматривает создание максимально благоприятных условий в учебной, бытовой и досуговой сфере деятельности студентов. Она охватывает основной бюджет времени студента и включает как учебное, так и внеучебное время.

Организация культурно-массовых мероприятий и развитие системы досуга; организация профилактической и превентивной работы по предупреждению правонарушений, наркомании и прочих асоциальных проявлений; воспитание у студентов чувства патриотизма, уважения и любви к своему факультету, вузу, выбранной профессии; повышение культуры и этики поведения студентов; повышение уровня нравственности, культуры, гражданского долга и гуманизма студентов; спортивно-оздоровительная работа и пропаганда здорового образа жизни и физической культуры, развитие студенческого самоуправления, участие обучающихся в работе общественных организаций, деятельности предприятий туристской индустрии, спортивных и творческих клубов, научных студенческих обществ, содействуют наряду с профессиональной подготовкой, нравственному, эстетическому и физическому совершенствованию, творческому развитию личности.

Согласно утвержденной в университете системе внутреннего контроля качества осуществляется трехуровневое управление воспитательной деятельностью: вуз – факультет – кафедра, а реализуемая личностно-ориентированная модель образования обеспечивает не только качественное образование, но и индивидуальное развитие, успешную социализацию каждого студента; создание наиболее благоприятных условий развития для всех студентов с учетом различий способностей.

7. Нормативно-методическое обеспечение системы оценки качества

освоения обучающимися ОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность по профилю подготовки «Организация и технология защиты информации»

В соответствии с ФГОС ВО бакалавриата по направлению подготовки 10.03.01 Информационная безопасность по профилю подготовки «Организация и технология защиты информации» и Типовым положением о вузе, оценка качества освоения обучающимися основных образовательных программ включает текущий контроль успеваемости, промежуточную и итоговую государственную аттестацию обучающихся.

Нормативно-методическое обеспечение текущего контроля успеваемости и промежуточной аттестации обучающихся по ОП бакалавриата осуществляется в соответствии с нормативно-методическими документами университета.

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

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей ОП вуз провел работу по созданию фондов оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации. Эти фонды включают: контрольные вопросы и типовые задания для практических занятий, лабораторных и контрольных работ, коллоквиумов, зачетов и экзаменов; тесты и компьютерные тестирующие программы; примерную тематику курсовых работ, рефератов и т.п., а также иные формы контроля, позволяющие оценить степень сформированности компетенций обучающихся.

7.2. Итоговая государственная аттестация выпускников ОП бакалавриата

Итоговая аттестация выпускника высшего учебного заведения является обязательной и осуществляется после освоения образовательной программы в полном объеме.

Итоговая государственная аттестация по направлению подготовки 10.03.01 Информационная безопасность по профилю подготовки «Организация

и технология защиты информации» включает сдачу государственного экзамена и защиту бакалаврской выпускной квалификационной работы.

Согласно Положению об итоговой государственной аттестации выпускников высших учебных заведений Российской Федерации, требованиям ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность по профилю подготовки «Организация и технология защиты информации» разработаны и утверждены требования к содержанию, объему и структуре выпускных квалификационных работ, а также требования к содержанию и процедуре проведения государственного экзамена.

8.Материалы, подтверждающие участие работодателей в разработке и реализации ОП

Доля преподавателей (в приведенных к целочисленным значениям ставок) из числа действующих руководителей и работников профильных организаций (имеющих стаж работы в данной профессиональной области не менее 3 лет) в общем числе преподавателей, обеспечивающих образовательный процесс по образовательным программам, регламентируется соответствующим ФГОС ВО.

При разработке ОП с учетом ПС и квалификационных требований к специалисту, целесообразно привлекались представителей работодателей и объединений работодателей. На ОП получены:

- рецензия от работодателя с краткой характеристикой реализуемой ОП и описанием формируемых у выпускника общекультурных и профессиональных компетенций;
- апробация на ФОС;
- предложения о включении дисциплин в учебный план.

9. Документы, регламентирующие содержание и организацию воспитательного процесса при реализации образовательной программы

В соответствии с положением Федерального закона от 31 июля 2020 г. №304-ФЗ «О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» по вопросам воспитания обучающихся» рабочая программа воспитания и календарный план воспитательной работы являются частью основной профессиональной образовательной программы, разрабатываемой и реализуемой в соответствии с действующим федеральным государственным образовательным стандартом. Рабочая программа воспитания по ОПОП и Календарный план воспитательной работы по ОПОП разработаны на основе Положения о рабочей программе воспитания и календарном плане воспитательной работы по основной профессиональной

образовательной программе бакалавриата, специалитета, подготовки специалистов и среднего звена в ФГБОУ ВО «МГТУ»

9.1. Рабочая программа воспитания по ОПОП

Рабочая программа воспитания как часть основной образовательной программы, реализуемой в образовательной организации высшего образования, разработана на период реализации образовательной программы и определяет комплекс ключевых характеристик системы воспитательной работы, проводимой с обучающимися по ОПОП (принципы, методологические подходы, цель, задачи, направления, формы, средства и методы воспитания, планируемые результаты и др.).

В рабочей программе воспитания определены основные принципы, методологические подходы, цель, задачи, направления, формы, средства и методы воспитания, планируемые результаты и др. с учетом приоритетных видов деятельности, обучающихся по направлению подготовки.

В рабочей программе воспитания указаны ресурсы реализации воспитательной деятельности (кадровые, организационные, материальные), соответствие воспитательным задачам инфраструктурных подразделений университета, а также формы взаимодействия с внешними организациями, социальными институтами и субъектами воспитания.

В рабочей программе воспитания определено соответствие видов воспитательной работы с формируемыми компетенциями в ходе освоения учебных дисциплин ОПОП. Рабочая программа воспитания утверждена на научно-методическом совете направления подготовки 10.03.01 Информационная безопасность и одобрена научно-методической комиссией факультета информационных систем в экономике и юриспруденции ФГБОУ ВО «МГТУ».

При разработке рабочей программы воспитания ОПОП взят за основу комплекс методологических подходов к организации воспитательной деятельности в рамках реализации ОПОП:

– аксиологический (ценностно-ориентированный) подход, который имеет гуманистическую направленность и предполагает, что в основе управления воспитательной системой при реализации лежит созидательная, социально-направленная деятельность, имеющая в своем осевом основании опору на стратегические ценности (ценность жизни и здоровья человека; духовно-нравственные ценности; социальные ценности; ценность общения, контакта и диалога; ценность развития и самореализации; ценность опыта самостоятельности и ценность профессионального опыта; ценность дружбы; ценность свободы и ответственности и др.), обладающие особой важностью и способствующие объединению, созиданию людей, разделяющих эти ценности;

– системный подход, который предполагает рассмотрение воспитательной системы по ОПОП как открытой социально-психологической, динамической, развивающейся системы, состоящей из двух взаимосвязанных подсистем: управляющей (руководство Университета: проректор по УР и проректор по социально-бытовой и воспитательной работе, заместители деканов по воспитательной работе, куратор академической группы, преподаватель) и управляемой (студенческое сообщество, студенческий актив, студенческие коллективы, студенческие группы и обучающиеся), что подчеркивает иерархичность расположения элементов данной системы и наличие субординационных связей между субъектами, их подчиненность и соподчиненность согласно особому месту каждого из них в системе;

– системно-деятельностный подход, позволяющий установить уровень целостности воспитательной системы, а также степень взаимосвязи ее подсистем в образовательном процессе, который является основным процессом, направленным на конечный результат активной созидательной воспитывающей деятельности педагогического коллектива;

– культурологический подход, который способствует реализации культурной направленности образования и воспитания, позволяет рассматривать содержание учебной и внеучебной деятельности как интегративную культуру в единстве ее аксиологического, системно-деятельностного и личностного компонентов. Культурологический подход направлен на: создание в Университете в рамках реализации ОПОП культуросообразной среды и организационной культуры; повышение общей культуры обучающихся, формирование их профессиональной культуры и культуры труда;

– проблемно-функциональный подход позволяет осуществлять целеполагание с учетом выявленных воспитательных проблем и рассматривать управление системой воспитательной работы в рамках реализации ОПОП как процесс взаимосвязанных, выполняемых одновременно или в некоторой последовательности управленческих функций (анализ, планирование, организация, регулирование, контроль), сориентированных на достижение определенных целей;

– научно-исследовательский подход рассматривает воспитательную работу по ОПОП как деятельность, имеющую исследовательскую основу, формирующую у обучающихся научного мировоззрения, развития научного мышления и познавательной самостоятельности;

– проектный подход предполагает разрешение имеющихся социальных и иных проблем посредством индивидуальной или совместной проектной или проектно-исследовательской деятельности обучающихся под руководством преподавателя;

– ресурсный подход учитывает готовность Университета реализовать систему воспитательной работы через нормативно-правовое, кадровое, финансовое, информационное, научно-методическое, учебно-методическое и материально-техническое обеспечение;

– здоровье сберегающий подход направлен на повышение культуры здоровья, сбережение здоровья субъектов образовательных отношений, что предполагает активное субъект-субъектное взаимодействие членов коллектива, реализующих ОПОП: по созданию здоровьеформирующей и здоровьесберегающей образовательной среды, по смене внутренней позиции личности в отношении здоровья на сознательно-ответственную, по развитию индивидуального стиля здоровьесозидающей деятельности преподавателей,

по разработке и организации здоровьесозидающих мероприятий и методического арсенала здоровьесберегающих занятий, по актуализации и реализации здорового образа жизни;

– информационный подход рассматривает воспитательную работу по ОПОП как информационный процесс, состоящий из специфических операций: по сбору и анализу информации о состоянии управляемого объекта; доведение информации до участников образовательного процесса с учетом принятия управленческого решения.

Воспитательная деятельность в рамках реализуемой ОПОП осуществляется по следующим направлениям воспитания:

– деятельность, направленная на развитие личности, создание условий для самоопределения и социализации обучающихся;

– деятельность, направленная на формирование у обучающихся чувства патриотизма и гражданственности;

– деятельность, направленная на формирование у обучающихся чувства уважения к памяти защитников Отечества и подвигам героев Отечества;

– деятельность, направленная на формирование у обучающихся уважения человеку труда и старшему поколению;

– деятельность, направленная на формирование у обучающихся уважения к закону и правопорядку;

– деятельность, направленная на формирование у обучающихся бережного отношения к культурному наследию и традициям многонационального народа Российской Федерации;

– деятельность, направленная на формирование у обучающихся правил и норм поведения в интересах человека, семьи, общества и государства;

– деятельность, направленная на формирование у обучающихся бережного отношения к природе и окружающей среде;

– деятельность, направленная на профилактику деструктивного поведения обучающихся.

Перечисленные направления, отражающие специфику и особенности воспитательной и образовательной деятельности по ОПОП, отражаются в рабочих программах дисциплин.

Воспитательная работа по ОПОП включена в рабочие программы дисциплин по приоритетным и вариативным направлениям в соответствующих темах и разделах дисциплины.

9.2. Календарный план воспитательной работы по ОПОП

Календарный план воспитательной работы по направлению подготовки 10.03.01 Информационная безопасность конкретизирует перечень событий и мероприятий воспитательной направленности, которые организуются и проводятся образовательной организацией и (или) в которых субъекты воспитательного процесса принимают участие.

В календарном плане воспитательной работы по направлению подготовки 10.03.01 Информационная безопасность отображается логическая последовательность научно-образовательных мероприятий, направленных на формирование у обучающихся качеств гармонично развитой личности в духовно-нравственном, гражданско-патриотическом направлениях.

Календарный план составлен на весь срок обучения, интегрирует мероприятия воспитательного характера, планируемые при реализации дисциплин учебного плана в рабочих программах дисциплин (модулей), обеспечивающих образовательный процесс по ОПОП СПО.

Календарный план содержит следующие пункты: дата, место, время и формат проведения; название мероприятия и организатор; форма проведения мероприятия; ответственный; количество участников; достижения обучающихся.

Мероприятия календарного плана сгруппированы по следующим модулям:

Модуль 1. Проектная и проектно-исследовательская деятельность обучающихся.

Модуль 2. Волонтерская (добровольческая) деятельность обучающихся.

Модуль 3. Учебно-исследовательская и научно-исследовательская деятельность.

Модуль 4. Студенческое международное сотружничество.

Модуль 5. Деятельность и виды студенческих объединений.

Модуль 6. Досуговая, творческая и социально-культурная деятельность по организации и проведению значимых событий и мероприятий.

Модуль 7. Вовлечение обучающихся в профориентационную деятельность.

Модуль 8. Вовлечение обучающихся в предпринимательскую деятельность.

10. Другие нормативно-методические документы и материалы, обеспечивающие качество подготовки обучающихся:

программа организации инклюзивного образования в ФГБОУ ВО «МГТУ» для инвалидов и лиц с ОВЗ.