

**ГАОУ ВО «Дагестанский государственный университет  
народного хозяйства»**

*Утверждена решением  
Ученого совета ДГУНХ,  
протокол № 11  
от 06 июня 2023 г*

**Кафедра «Информационные технологии и  
информационная безопасность»**

**РАБОЧАЯ ПРОГРАММА ПРЕДДИПЛОМНОЙ  
ПРАКТИКИ**

**Специальность 10.02.05 Обеспечение  
информационной безопасности автоматизированных  
систем**

**Квалификация – техник по защите информации**

**Форма обучения – очная**

**Махачкала – 2023**

**УДК 004.056.5**

**ББК 32.973.2**

**Составитель** – Гасанова Зарема Ахмедовна, кандидат педагогических наук, доцент кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

**Внутренний рецензент** – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

**Внешний рецензент** – Газимагомедов Ахмед Абдуллаевич, кандидат экономических наук, ведущий инженер-программист Дагестанского федерального исследовательского центра академии наук.

**Представитель работодателя** – Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза».

*Рабочая программа преддипломной практики разработана в соответствии с требованиями федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённого приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г., № 1553, в соответствии с приказом Минпросвещения России от 24.08.2022 г., № 762 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования», с приказом Министерства науки и высшего образования Российской Федерации и Министерства просвещения Российской Федерации от 5 августа 2020 г. № 885/390 «О практической подготовке обучающихся».*

Рабочая программа преддипломной практики размещена на официальном сайте [www.dgunh.ru](http://www.dgunh.ru)

Гасанова З.А. Рабочая программа преддипломной практики для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. – Махачкала: ДГУНХ, 2021 г., 23 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 05 июня 2023 г.

Рекомендована к утверждению руководителем образовательной программы СПО – программы подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, к.пед.н., Гасановой З.А.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 31 мая 2023 г., протокол № 10.

## Содержание

	Стр.
1. Вид практики, способ и форма ее проведения.....	4
2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.....	5
3. Место в структуре образовательной программы.....	12
4. Объем практики в зачетных единицах и ее продолжительность в неделях либо в академических часах.....	12
5. Содержание практики.....	12
6. Форма отчетности по практике.....	14
7. Оценочные материалы для проведения промежуточной аттестации обучающихся по практике.....	14
8. Перечень учебной литературы и ресурсов сети "Интернет", необходимых для проведения практики.....	17
9. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных, используемых при проведении практики .....	21
10. Материально-техническая база, необходимая для проведения практики.....	22
Лист актуализации рабочей программы.....	23

## **1. Вид практики, способ и формы ее проведения.**

Практика обучающихся является составной частью основной профессиональной образовательной программы высшего образования при подготовке магистров. Практика осуществляется в целях формирования и закрепления профессиональных знаний, умений и навыков, полученных в результате теоретической подготовки, а также для изучения производственного опыта, приобретения организаторских навыков работы и формирования системы ключевых компетенций.

**Вид практики** – производственная практика.

**Тип практики** – преддипломная практика.

**Способы проведения практики** – стационарная и выездная.

**Форма проведения практики** – дискретная, путем выделения непрерывного периода учебного времени для проведения практики.

**Место проведения практики.**

Практика проводится в организациях или на предприятиях любых организационно-правовых форм, с которыми у ГАОУ ВО «Дагестанский государственный университет народного хозяйства» заключен договор об организации проведения практики обучающихся, а также в структурных подразделениях ГАОУ ВО «Дагестанский государственный университет народного хозяйства».

Местом прохождения преддипломной практики являются организации, имеющие разветвленную структуру, использующие многофункциональные информационные системы, которые нуждаются в администрировании и защите информации.

Распределение студентов в профильные организации осуществляется кафедрой, на основе выбранной им темы выпускной квалификационной работы.

Направление на практику оформляется приказом ректора Университета с указанием закрепления каждого обучающегося за организацией, а также с указанием вида и срока прохождения практики.

Обучающиеся, совмещающие обучение с трудовой деятельностью, вправе проходить практику по месту трудовой деятельности в случаях, если профессиональная деятельность, осуществляемая ими, соответствует требованиям к содержанию практики и теме выпускной квалификационной работы.

Выбор мест прохождения практик для лиц с ограниченными возможностями здоровья производится с учетом состояния здоровья обучающихся и требований по доступности.

Практика может быть организована полностью или частично с применением электронного обучения, дистанционных образовательных технологий без непосредственного нахождения обучающегося на рабочем месте в профильной организации/учебном подразделении ДГУНХ в формате дистанционной (удаленной) работы при опосредованном (на расстоянии) взаимодействии с руководителями практики как со стороны университета, так и со стороны профильной организацией.

Прохождение практики предусматривает, в том числе при опосредованном (на расстоянии) взаимодействии:

- Контактную работу: групповые консультации, зачет – 3 академических часа;
- иную форму работы студента во время практики (работа во взаимодействии с руководителем от профильной организации – 321 академический час).

## **2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.**

Целями преддипломной практики являются: приобретение учащимися практических навыков и компетенций в сфере профессиональной деятельности и подготовка выпускной квалификационной работы.

Основными задачами преддипломной практики являются:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;
- администрирование подсистем информационной безопасности объекта;
- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;
- проведение предварительного технико-экономического обоснования проектных расчетов;
- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств;
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

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

Ознакомиться с:

- с используемыми в подразделении методами анализа технологии обработки данных в распределенных системах с целью оптимизации их производительности и повышения надежности функционирования;
- с типовыми методами проектирования и оценки эффективности сложных систем в области деятельности подразделения.

Изучить:

- методы применения системного подхода к обеспечению информационной безопасности в различных сферах деятельности подразделения;
- в рамках задач обеспечения информационной безопасности с применяемыми в подразделении подходами к решению вопросов использования радиоэлектронной аппаратуры и других технических средств.

Приобрести практические навыки:

- использования современных средств разработки программного обеспечения, на языках высокого уровня и языках СУБД, библиотеки объектов и классов для решения задач создания и сопровождения автоматизированных систем;
- применения стандартных криптографических решений для защиты информации и квалифицированно оценивать их качество;
- в реализации системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем.

<i><b>Код компетенции</b></i>	<i><b>Формулировка компетенции</b></i>
<b>Общекультурные компетенции</b>	
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.
<b>Профессиональные компетенции</b>	
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.
ПК 4.1.	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения
ПК 4.2.	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3.	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
ПК 4.4.	Обеспечивать применение средств защиты информации в компьютерной системе

### **3. Место практики в структуре образовательной программы**

Преддипломная практика является составной частью ОПОП ВО – программы магистратуры по направлению подготовки 10.02.05 Информационная безопасность, профилю «Управление информационной безопасностью и технологии защиты информации» и в полном объеме относится к части, формируемой участниками образовательных отношений.



Преддипломная практика является обязательным этапом обучения специалиста по специальности **10.02.05 Обеспечение информационной безопасности автоматизированных систем.**

Преддипломная практика является важнейшим элементом учебного процесса на заключительном этапе обучения. Она обеспечивает закрепление и расширение знаний, полученных при изучении теоретических дисциплин, овладение навыками практической работы, приобретение опыта работы в трудовом коллективе, выполнение выпускной квалификационной работы.

#### **4. Объем практики в зачетных единицах и продолжительность в неделях или в академических часах**

Общая трудоемкость преддипломной практики составляет 9 зачетных единиц.

Продолжительность практики составляет 6 недель.

Результаты прохождения практики оцениваются посредством проведения промежуточной аттестации в виде защиты отчета по практике.

При реализации производственной практики образовательная деятельность организована в форме практической подготовки.

#### **5. Содержание практики.**

<i>№ п/ п</i>	<i>Разделы (этапы) практики</i>	<i>Виды работ обучающегося на практике</i>	<i>Формы отчетнос ти по практике</i>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>
1	<b>Подготовительный этап: Общие сведения об организации - базе практики</b>	Инструктаж по технике безопасности, правилам внутреннего распорядка организации и правилам охраны труда	Отчет по практике, дневник
2		Обсуждение совместного рабочего графика (плана) проведения практики с руководителем практики от производства, порядок его реализации	Отчет по практике, дневник
3		Изучение технологии работы объекта практики	Отчет по практике, дневник
4		Анализ нормативных и правовых актов предприятия/организации	Отчет по практике, дневник
5		Анализ информационных средств и компьютерных программ, применяемых на предприятии/организации	Отчет по практике, дневник
6		<b>Основной этап: Сбор</b>	Анализ исходных данных для

	<b>материала для выполнения выпускной квалификационной работы</b>	проектирования системы информационной безопасности на объекте практики	практике, дневник	
7		Мониторинг работоспособности и анализ эффективности мер, реализуемых на объекте практики	Отчет по практике, дневник	
8		Работа с технической литературой и нормативными и правовыми документами	Отчет по практике, дневник	
9		Формирование комплекса мер по обеспечению информационной безопасности на объекте практики	Отчет по практике, дневник	
10		Разработка подсистем управления информационной безопасностью	Отчет по практике, дневник	
11		Оформление рабочей документации с учетом действующих нормативной и технической документации	Отчет по практике, дневник	
12		Формирование требований политики безопасности на объекте практики и ее реализация	Отчет по практике, дневник	
13		Выполнение индивидуального задания	Отчет по практике, дневник	
14		<b>Заключительный этап: Промежуточная аттестация</b>	Систематизация материала, подготовка отчета	Отчет по практике, дневник, аттестационный лист

## 6. Формы отчетности по практике

Формы отчетности по практике:

- дневник по практике;
- аттестационный лист;
- характеристика на студента;
- отчет обучающегося по практике.

Дневник по практике включает в себя индивидуальное задание для обучающегося, выполняемое в период практики; рабочий график (план) проведения практики; ежедневные краткие сведения о проделанной работе, каждая запись о которой должна быть завизирована руководителями практики. Дневник заполняется в ходе практики, с ним обучающийся должен явиться в профильную организацию.

Аттестационный лист по практике содержит сведения по оценке освоенных обучающимся в период прохождения практики общекультурных,

общефессиональных, профессиональных компетенций. Аттестационный лист заполняется и подписывается руководителем практики от Университета.

Характеристика на обучающегося, проходившего практику заполняется и подписывается руководителем практики от профильной организации. Характеристика содержит оценку профессиональных навыков обучающихся, рекомендации по совершенствованию профессиональной подготовки студента, а также рекомендуемую оценку.

Отчет по практике представляет собой итоговый письменный отчет, составленный в ходе практики. Цель отчета – показать степень полноты выполнения обучающимся программы и задания практики. В отчете отражаются итоги деятельности обучающихся во время прохождения практики в соответствии с разделами и позициями задания, соответствующие расчеты, анализ, обоснования, выводы и предложения.

## **7. Оценочные материалы для проведения промежуточной аттестации обучающихся по практике**

Результаты прохождения практики оцениваются посредством проведения промежуточной аттестации. Формой промежуточной аттестации обучающихся по практике является зачет с оценкой. По результатам проверки отчетной документации и собеседования выставляется зачет с оценкой. Неудовлетворительные результаты промежуточной аттестации по практике или непрохождение промежуточной аттестации по практике при отсутствии уважительных причин признаются академической задолженностью.

Промежуточная аттестация по итогам практики проводится комиссией по проведению промежуточной аттестации, в состав которой помимо руководителя практики могут включаться педагогические работники кафедры, по которой обучающимися осуществляется прохождение соответствующей практики, представители организаций и предприятий, на базе которых проводилась практика, с занесением результатов в экзаменационную ведомость и в зачетную книжку обучающегося.

При выставлении оценки учитываются содержание, качество отчета по практике, правильность и полнота ответов на вопросы, задаваемые во время процедуры защиты отчета, характеристика руководителя от профильной организации, оценка, данная обучающемуся руководителем практики от ДГУНХ в аттестационном листе.

Каждому студенту задаются вопросы по всем разделам практики.

### **Примерные индивидуальные задания для выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью**

1. Анализ автоматизированной системы защиты конфиденциальной информации на основе программного обеспечения с открытым исходным кодом;

2. Анализ системы защиты информации телекоммуникационной сети предприятия;
3. Разработка организационно-распорядительных документов по защите информации в автоматизированных системах;
4. Разработка автоматизированной системы защищенного электронного документооборота;
5. Анализ уязвимостей внедряемой системы защиты информации;
6. Разработка проекта системы управления доступом удаленных компьютеров, подключенных к сети Internet;
7. Установка и настройка средств защиты информации в автоматизированных системах;
8. Разработка программного комплекса оценки соответствия автоматизированной системы требованиям безопасности информации;
9. Разработка метода защиты персональных данных при использовании веб-технологий;
10. Аудит защищенности информации в автоматизированных системах
11. Разработка комплекса оценки защищенности информации в информационной системе обработки персональных данных;
12. Разработка программного обеспечения автоматизированного средства защиты информации;
13. Разработка и реализация политики информационной безопасности предприятия.
14. Мониторинг защищенности информации в автоматизированных системах

Каждому студенту задаются вопросы по всем разделам практики.

**Примерный перечень вопросов:**

- каковы должностные обязанности сотрудников отдела информационной безопасности?
- какими качествами должен обладать специалист по информационной безопасности?
- какие методики оценки рисков вам известны?
- какие управленческие теории вами были использованы?
- приведите примеры ведущих отечественных авторов и изданий, которые были использованы при проведении исследования
- какие зарубежные научные издания были использованы при проведении исследования?
- приведите пример требований к порядку проведения работ в рассматриваемой организации?
- какие нормативно-правовые акты регуляторов в области информационной безопасности вы использовали?

- какие параметры защиты были применены в настройках операционных систем в организации?

- какие из используемых программных средств сертифицированы ФСТЭК/ФСБ России?

- каковы параметры частной политики безопасности в информационных системах организации?

- какие меры для обеспечения информационной безопасности информационных систем вы рекомендуете применить в организации?

- какие виды конфиденциальной информации используются в организации?

- каким нормативным документом, регламентирующим требования безопасности, необходимо руководствоваться при аттестации информационных систем организации?

- по каким показателям осуществлялась классификация информационных систем?

- каковы требования к защите для установленного класса систем?

- какие нормативные и методические документы регламентируют оформление технических документов?

- какие отечественные и зарубежные стандарты в области компьютерной безопасности были изучены и использованы в работе?

- какие нормативно-правовые системы и др. источники информации вы использовали

- какие регламентные и проверочные работ по проверке соблюдения требований стандартов в области информационной безопасности были проведены вами?

- какие методики оценки защищенности информации были применены?

- охарактеризуйте уровни политики безопасности организации?

- какие документы регламентируют систему менеджмента информационной безопасности?

- какие технологии обеспечения защиты информации в компьютерных сетях используются в организации?

- какие предложения по совершенствованию системы управления защиты информации автоматизированных систем организации вы можете дать?

Методические материалы, определяющие процедуры оценивания умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе прохождения практики, позволяющие оценить уровень сформированности компетенций, содержатся в приложении к ООП ВО – программе магистратуры по направлению подготовки 10.02.05 Информационная безопасность, профиля «Управление информационной безопасностью и технологии защиты информации».

## 8. Перечень учебной литературы и ресурсов сети "Интернет", необходимых для проведения практики.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам и к электронной информационно-образовательной среде университета (<http://e-dgunh.ru>). Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивает возможность доступа обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

### 8.1. Перечень основной и дополнительной учебной литературы, необходимой для проведения практики

№ п/п	Автор	Название основной и дополнительной учебной литературы, необходимой для проведения практики	Выходные данные	Количество экземпляров в библиотеке ДГУНХ/адрес доступа
<b>Основная учебная литература</b>				
1.	Аверченков, В.И.	Аудит информационной безопасности : учебное пособие для вузов	Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6	<a href="https://biblioclub.ru/index.php?page=book_read&amp;id=93245&amp;sr=1">https://biblioclub.ru/index.php?page=book_read&amp;id=93245&amp;sr=1</a>
2.	Веселов, Г.Е.	Менеджмент риска информационной безопасности	Таганрог : Издательство Южного федерального университета, 2016. - 109 с.	<a href="https://biblioclub.ru/index.php?page=book_read&amp;id=493331&amp;sr=1">https://biblioclub.ru/index.php?page=book_read&amp;id=493331&amp;sr=1</a>
3.	Пелешенко, В.С.	Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления	Ставрополь : СКФУ, 2017. - 86 с.	<a href="https://biblioclub.ru/index.php?page=book_read&amp;id=467139&amp;sr=1">https://biblioclub.ru/index.php?page=book_read&amp;id=467139&amp;sr=1</a>
4.	Аверченков, В.И.	Служба защиты информации:	Москва : Издательство	<a href="https://">https://</a>

		организация и управление	«Флинта», 2016. - 186 с. ISBN 978-5-9765-1271-9	<a href="http://biblioclub.ru/index.php?page=book_read&amp;id=93356&amp;sr=1">biblioclub.ru/index.php?page=book_read&amp;id=93356&amp;sr=1</a>
5.	Голиков А. М.	Основы проектирования защищенных телекоммуникационных систем: учебное пособие	Томск: ТУСУР, 2016. – 396 с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=480796">http://biblioclub.ru/index.php?page=book&amp;id=480796</a>
6.	Кияев В., Граничин О.	Безопасность информационных систем	М.:Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=429032">http://biblioclub.ru/index.php?page=book&amp;id=429032</a>
7.	Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков	Программно-аппаратные средства защиты информационных систем: учебное пособие	Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2017. – 194 с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=499013">http://biblioclub.ru/index.php?page=book&amp;id=499013</a>
8.	Долозов Н. Л., Гулятьева Т. А.	Программные средства защиты информации: конспект лекций	Новосибирск: НГТУ, 2015. - 63 с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=438307">http://biblioclub.ru/index.php?page=book&amp;id=438307</a>
9.	Голиков А. М.	Основы проектирования защищенных телекоммуникационных систем: учебное пособие	Томск: ТУСУР, 2016. – 396 с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=480796">http://biblioclub.ru/index.php?page=book&amp;id=480796</a>
10.	-	Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суоров	Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=428820">http://biblioclub.ru/index.php?page=book&amp;id=428820</a>
11.	Мэйволд Э.	Безопасность сетей	Москва : Национальный Открытый	<a href="http://biblioclub.ru/index.php?">http://biblioclub.ru/index.php?</a>

			Университет «ИНТУИТ», 2016. - 572 с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=429035">page=book&amp;id=429035</a>
<b>Дополнительная учебная литература</b>				
<b><i>а) Дополнительная учебная литература</i></b>				
1.	А.В. Душкин, О.В. Ланкин, С.В. Потехецкий и др.	Методологические основы построения защищенных автоматизированных систем: учебное пособие	Воронеж: Воронежская государственная лесотехническая академия, 2013. - 258с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=255851">http://biblioclub.ru/index.php?page=book&amp;id=255851</a>
2.	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=438331">http://biblioclub.ru/index.php?page=book&amp;id=438331</a>
3.		Построение коммутируемых компьютерных сетей / Е.В. Смирнова, И.В. Баскаков, А.В. Пролетарский, Р.А. Федотов	Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 429 с.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=429834">http://biblioclub.ru/index.php?page=book&amp;id=429834</a>
4.	Проскураков А.В.	Компьютерные сети: основы построения компьютерных сетей и телекоммуникаций с.	Министерство науки и высшего образования Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», Инженерно-технологическая академия. –	<a href="http://biblioclub.ru/index.php?page=book&amp;id=561238">http://biblioclub.ru/index.php?page=book&amp;id=561238</a>



			Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. – 202	
<b>Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ</b>				
<ol style="list-style-type: none"> <li>1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями).</li> <li>2. ГОСТ 34.320-96. Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы. 2001 г. <a href="http://www.standartgost.ru">www.standartgost.ru</a></li> <li>3. ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г. <a href="http://www.standartgost.ru">www.standartgost.ru</a></li> <li>4. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. <a href="http://www.standartgost.ru">www.standartgost.ru</a></li> <li>5. ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование. 2005 г. <a href="http://www.standartgost.ru">www.standartgost.ru</a></li> <li>6. ГОСТ Р ИСО/МЭК ТО 16326-2002. Программная инженерия. Руководство по применению ГОСТ Р ИСО/МЭК 12207 при управлении проектом. 2002 г. <a href="http://www.standartgost.ru">www.standartgost.ru</a></li> <li>7. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г. <a href="http://www.standartgost.ru">www.standartgost.ru</a></li> </ol>				
<b>В) Периодические издания</b>				
<ol style="list-style-type: none"> <li>1. Журнал для пользователей персональных компьютеров «Мир ПК»</li> <li>2. Научный журнал «Информатика и ее применение»</li> <li>3. Информатика и безопасность</li> <li>4. Журнал о компьютерах и цифровой технике «Computer Bild»</li> <li>5. Рецензируемый научный журнал «Информатика и система управления»</li> <li>6. Рецензируемый научный журнал «Проблемы информационной безопасности»</li> </ol>				
<b>Г) Справочно-библиографическая литература</b>				
<ol style="list-style-type: none"> <li>1. Краткий энциклопедический словарь по информационной безопасности : словарь / сост. В.Г. Дождиков, М.И. Салтан. – Москва : Энергия, 2010. – 240 с. <a href="http://biblioclub.ru/index.php?page=book&amp;id=58393">http://biblioclub.ru/index.php?page=book&amp;id=58393</a></li> </ol>				

## 8.2. Перечень ресурсов сети «Интернет», необходимых для проведения практики

Перечень ресурсов сети "Интернет", необходимых для проведения практики:

1. <http://www.fsb.ru/> – официальный сайт ФСБ
2. <http://fstec.ru/> – официальный сайт ФСТЭК
3. <http://www.consultant.ru/> – онлайн-версия информационно-правовой системы "КонсультантПлюс"
4. <http://Standartgost.ru> - Открытая база ГОСТов
5. <http://rkn.gov.ru/> Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;

Для самостоятельного изучения материала и ознакомления с новинками в области информационной безопасности рекомендуется использовать следующие Интернет-ресурсы:

6. <http://www.infotechs.ru> - Сайт компании "Инфотекс"
7. <http://citforum.ru/> - IT-портал «Сервер Информационных Технологий»;
8. <https://habrahabr.ru/> - ресурс для IT-специалистов, издаваемый компанией «ТМ»;
9. <http://stackoverflow.com/> - сайт вопросов и ответов для IT-специалистов.

## **9. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных, используемых при проведении практики.**

### **9.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства:**

- Windows 10
- Microsoft Office Professional
- Adobe Acrobat Reader DC
- VLC Media player
- 7-zip
- Программные и программно-аппаратные средства защиты информации, эксплуатируемые в организации.

### **9.2. Перечень информационных справочных систем и профессиональных баз данных:**

- информационно справочная система «Консультант+».

### **9.3. Перечень профессиональных баз данных:**

- Открытая база ГОСТов ([www.standartgost.ru](http://www.standartgost.ru))
- Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (<https://fstec.ru/%20tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sszi>).
- Перечень средств защиты информации, сертифицированных ФСБ России. (<http://clsz.fsb.ru/certification.htm>);
- Единый реестр российских программ для электронных вычислительных машин и баз данных

(<https://reestr.minsvyaz.ru/reestr/>).

- Банк данных угроз безопасности информации ([bdu.fstec.ru](http://bdu.fstec.ru)).
- Национальная база данных уязвимостей ([www.nvd.nist.gov](http://www.nvd.nist.gov)).
- Реестр операторов, осуществляющих обработку персональных данных (<https://rkn.gov.ru/personal-data/register/>).

#### **10. Материально-техническая база, необходимая для проведения практики**

Необходимую материально-техническую базу практики обеспечивает профильная организация в соответствии с договором о практической подготовке обучающихся.

Для проведения консультаций и приема зачета по преддипломной практике используются следующие специальные помещения – учебные аудитории:

**Учебная аудитория для проведения учебных занятий № 4.11** (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)

##### ***Перечень основного оборудования:***

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, персональный компьютер (моноблок) с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» ([www.biblioclub.ru](http://www.biblioclub.ru)), ЭБС «ЭБС Юрайт» ([www.ura.it.ru](http://www.ura.it.ru)).

##### ***Перечень учебно-наглядных пособий:***

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

**Лист актуализации рабочей программы преддипломной практики**