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

Направление подготовки

10.04.01 Информационная безопасность,

профиль «Управление информационной безопасностью и технологии защиты информации»

Уровень высшего образования - магистратура

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 высшего образования по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 26 ноября 2021 г. № 1455, в соответствии с приказом Министерства науки и высшего образования от 6.04.2021 г., № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам магистратуры, программам специалитета, программам магистратуры», 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

Гасанова З.А. Рабочая программа преддипломной практики для направления подготовки 10.04.01 Информационная безопасность, профиль «Управление информационной безопасностью и технологии защиты информации». – Махачкала: ДГУНХ, 2023 г., 21 с.

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

Рекомендована к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

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

Содержание

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 – 213 академический часа).

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.

Процесс прохождения производственной практики направлен на формирование следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по направлению подготовки 10.04.01 Информационная безопасность, профилю «Управление информационной безопасностью и технологии защиты информации»:

код компетенции	формулировка компетенции
УК	**УНИВЕРСАЛЬНЫЕ КОМПЕТЕНЦИИ**

УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-1	Способен осуществлять подбор средств и технологий защиты информации и применять их в профессиональной деятельности
ПК-2	Способен осуществлять сбор, анализ и систематизацию научно-технической информации по вопросам обеспечения информационной безопасности объектов информатизации
ПК-3	Способен организовывать и обеспечивать защиту объектов информатизации, проводить аттестацию объектов информатизации по требованиям безопасности информации

В результате прохождения данной практики обучающийся должен приобрести следующие умения и практические навыки:

Код и наименование компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения при прохождении практики***	
		Умения	***Навыки или практический опыт деятельности***
УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	ИУК-6.1. Определяет образовательные потребности и способы совершенствования собственной деятельности	- определять образовательные потребности и способы совершенствования собственной	- определения образовательных потребностей и способы совершенствования собственной
	ИУК-6.2. Выбирает и реализует стратегию собственного развития в профессиональной сфере	- определять стратегию и траекторию собственного развития в профессиональной сфере	
ПК-1. Способен осуществлять подбор средств и технологий защиты	ИПК-1.1 Разрабатывает проектные решения по применяемым методам и средствам защиты	осуществлять подбор программно-аппаратных средств защиты исходя из существующих требований	установки, настройки средств защиты информации
	ИПК-1.2. Обеспечивает	классифицировать и	проведения

информации и применять их в профессиональной деятельности	безопасность применяемых информационных технологий	оценивать угрозы безопасности информации автоматизированной системы; разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы	анализа уязвимостей автоматизированных и информационных систем
ПК-2. Способен осуществлять сбор, анализ и систематизацию научно-технической информации по вопросам обеспечения информационной безопасности объектов информатизации	ИПК-2.1. Проводит анализ безопасности объектов информатизации	- осуществлять сбор, анализ и систематизацию научно-технической информации по вопросам обеспечения информационной безопасности объекта информатизации	проведения анализа безопасности компьютерных систем
	ИПК-2.2. Проводит анализ уязвимости программных и программно-аппаратных средств системы защиты информации и экспертизу состояния защищенности информации с использованием современного инструментария и интеллектуальных информационно-аналитических систем	- анализировать уязвимости программных и программно-аппаратных средств системы защиты информации и экспертизу состояния защищенности информации с использованием современного инструментария и интеллектуальных информационно-аналитических систем	- анализа уязвимости программных и программно-аппаратных средств системы защиты информации и экспертизу состояния защищенности информации с использованием современного инструментария и интеллектуальных

			информационно-аналитических систем
ПК-3. Способен организовывать и обеспечивать защиту объектов информатизации, проводить аттестацию объектов информатизации по требованиям безопасности информации	ИПК-3.1. Организует защиту объектов информатизации с учетом существующих нормативно-правовых и методических документов	- организовывать защиту объектов информатизации с учетом существующих нормативно-правовых и методических документов регуляторов	- анализа состояния защищенности информации объектов информатизации на соответствие существующим требованиям
	ИПК-3.2. Разрабатывает организационно-распорядительные и эксплуатационно-технические документы в системах обеспечения информационной безопасности	- определять состав и разрабатывать организационно-распорядительные документы по защите информации	- подготовки организационно-распорядительной документации определяющей правила и процедуры управления системой защиты информации
	ИПК-3.3. Разрабатывает систему защиты информации с учетом специфики деятельности организации и обрабатываемых данных	- разрабатывать систему защиты информации с учетом специфики деятельности организации и обрабатываемых данных	- пределения требований к системе защиты информации исходя их специфики деятельности организации и обрабатываемых данных

3. Место практики в структуре образовательной программы

Преддипломная практика является составной частью ОПОП ВО – программы магистратуры по направлению подготовки 10.04.01 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 магистра по направлению подготовки 10.04.01 Информационная безопасность, профилю «Управление информационной безопасностью и технологии защиты информации» и предусматривается учебным планом в Блоке 2 «Практики».

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 6 зачетных единиц.

Продолжительность практики составляет 4 недели.

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

Сроки практики для обучающихся определяются учебным планом и календарным учебным графиком по направлению подготовки 10.04.01 Информационная безопасность, профилю «Управление информационной безопасностью и технологии защиты информации».

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

5. Содержание практики.

№ п/п	*Разделы (этапы) практики*	*Виды работ обучающегося на практике*	*Формы отчетности по практике*
1	***2***	**3**	**4**
1	**Подготовительный этап: Общие сведения об организации - базе практики**	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	Отчет по

		актов предприятия/организации	практике, дневник
5		Анализ информационных средств и компьютерных программ, применяемых на предприятии/организации	Отчет по практике, дневник
6	**Основной этап: Сбор материала для выполнения выпускной квалификационной работы**	Анализ исходных данных для проектирования системы информационной безопасности на объекте практики	Отчет по 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	**Заключительный этап: Промежуточная аттестация**	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, общепрофессиональных, 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 применит 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 10.04.01 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
Основная учебная литература				
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	https://biblioclub.ru/index.php?page=book_red&id=93245&sr=1
2.	Веселов, Г.Е.	Менеджмент риска информационной безопасности	Таганрог : Издательство Южного федерального университета, 2016. - 109 с.	https://biblioclub.ru/index.php?page=book_red&id=493331&sr=1
3.	Пелешенко, В.С.	Менеджмент инцидентов	Ставрополь : СКФУ, 2017. -	https://

		информационной безопасности защищенных автоматизированных систем управления	86 с.	biblioclub.ru/index.php?page=book_red&id=467139&sr=1
4.	Аверченков, В.И.	Служба защиты информации: организация и управление	Москва : Издательство «Флинта», 2016. - 186 с. ISBN 978-5-9765-1271-9	https://biblioclub.ru/index.php?page=book_red&id=93356&sr=1
5.	Голиков А. М.	Основы проектирования защищенных телекоммуникационных систем: учебное пособие	Томск: ТУСУР, 2016. – 396 с.	http://biblioclub.ru/index.php?page=book&id=480796
6.	Кияев В., Граничин О.	Безопасность информационных систем	М.:Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с.	http://biblioclub.ru/index.php?page=book&id=429032
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.	http://biblioclub.ru/index.php?page=book&id=499013
8.	Долозов Н. Л., Гультяева Т. А.	Программные средства защиты информации: конспект лекций	Новосибирск: НГТУ, 2015. - 63 с.	http://biblioclub.ru/index.php?page=book&id=438307
9.	Голиков А. М.	Основы проектирования защищенных телекоммуникационных систем: учебное пособие	Томск: ТУСУР, 2016. – 396 с.	http://biblioclub.ru/index.php?page=book&id=480796
10.	-	Технологии защиты информации в компьютерных сетях / Н.А. Руденков,	Москва : Национальный Открытый Университет	http://biblioclub.ru/index.php?page=book&i

		А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов	«ИНТУИТ», 2016. - 369 с.	d=428820
11.	Мэйволд Э.	Безопасность сетей	Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.	http:// biblioclub.ru/ index.php? page=book&i d=429035
Дополнительная учебная литература				
а) Дополнительная учебная литература				
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.	http:// biblioclub.ru/ index.php? page=book&i d=255851
2.	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с.	http:// biblioclub.ru/ index.php? page=book&i d=438331
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.	http:// biblioclub.ru/ index.php? page=book&i d=429834
4.	Проскуряков 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	http:// biblioclub.ru/ index.php? page=book&i d=561238

			«Южный федеральный университет», Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. – 202	

Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями).
2. ГОСТ 34.320-96.Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы. 2001 г. www.standartgost.ru
3. ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г. www.standartgost.ru
4. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. www.standartgost.ru
5. ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование. 2005 г. *www.standartgost.ru*
6. ГОСТ Р ИСО/МЭК ТО 16326-2002. Программная инженерия. Руководство по применению ГОСТ Р ИСО/МЭК 12207 при управлении проектом. 2002 г. www.standartgost.ru
7. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г. www.standartgost.ru

В) Периодические издания

1. Журнал для пользователей персональных компьютеров «Мир ПК»
2. Научный журнал «Информатика и ее применение»
3. Информатика и безопасность
4. Журнал о компьютерах и цифровой технике «Computer Bild»
5. Рецензируемый научный журнал «Информатика и система управления»
6. Рецензируемый научный журнал «Проблемы информационной безопасности»

Г) Справочно-библиографическая литература

1. Краткий энциклопедический словарь по информационной безопасности :

словарь / сост. В.Г. Дождиков, М.И. Салтан. – Москва : Энергия, 2010. – 240 с. http://biblioclub.ru/index.php?page=book&id=58393

8.2. Перечь 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.infotecs.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)
- 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).
- Национальная база данных уязвимостей (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), ЭБС «ЭБС Юрайт» (www.urait.ru).

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

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

Лист актуализации рабочей программы преддипломной практики