

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

*Утверждена решением
Ученого совета ДГУНХ,
протокол № 13
от 06 июля 2020 г*

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

**РАБОЧАЯ ПРОГРАММА ПРЕДДИПЛОМНОЙ
ПРАКТИКИ**

Направление подготовки

10.03.01 Информационная безопасность,

профиль «Безопасность автоматизированных систем»

Уровень высшего образования - бакалавриат

Форма обучения – очная

Махачкала – 2020

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 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г., № 1515, в соответствии с приказом Минобрнауки РФ от 5.04.2017 г., № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, 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 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2020 г., 26 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 03 июля 2020 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» 30 июня 2020 г., протокол № 12

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.....	15
4. Объем практики в зачетных единицах и ее продолжительность в неделях либо в академических часах.....	15
5. Содержание практики.....	15
6. Форма отчетности по практике.....	17
7. Оценочные материалы для проведения промежуточной аттестации обучающихся по практике.....	17
8. Перечень учебной литературы и ресурсов сети "Интернет", необходимых для проведения практики.....	20
9. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных, используемых при проведении практики	24
10. Материально-техническая база, необходимая для проведения практики.....	25
Лист актуализации рабочей программы.....	26

1. Вид практики, способ и формы ее проведения.

Практика обучающихся является составной частью основной профессиональной образовательной программы высшего образования при подготовке бакалавров. 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 академических часов).

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 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем»:

код компетенции	формулировка компетенции
ОК	ОБЩЕКУЛЬТУРНЫЕ КОМПЕТЕНЦИИ
ОК-5	Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области

	обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.
ОК-6	Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия.
ОК-7	Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности.
ОК-8	Способность к самоорганизации и самообразованию.
ОПК	ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ
ОПК-5	Способность использовать нормативные правовые акты в профессиональной деятельности
ОПК-7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК	ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ
ПК-1	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.
ПК-2	Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.
ПК-3	Способность администрировать подсистемы информационной безопасности объекта защиты.
ПК-4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.
ПК-5	Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-6	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения

	информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК-8	Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
ПК-9	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.
ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.
ПК-11	Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов
ПК-12	Способность принимать участие в проведении экспериментальных исследований системы защиты информации
ПК-13	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
ПК-14	Способность организовать работу малого коллектива исполнителей в профессиональной деятельности
ПК-15	Способность организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ПСК	ПРОФЕССИОНАЛЬНЫЕ СПЕЦИАЛЬНЫЕ КОМПЕТЕНЦИИ
ПСК-1	Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации
ПСК-2	Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей

ПСК-3	Способность планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации
ПСК-4	Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности

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

Формируемые компетенции	Планируемые результаты обучения при прохождении практики	
	Умения	Навыки или практический опыт деятельности
ОК-5: Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	соблюдать нормы профессиональной этики	владения профессиональной терминологией в области информационной безопасности
ОК-6: Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия.	формулировать индивидуальные, групповые и организационные цели; оценивать эффективность управленческих решений в области защиты информации;	работы в коллективе, в том числе в качестве лидера
ОК-7: Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного	читать и переводить научно-техническую литературу на иностранном языке по	создания на русском языке грамотных и логически непротиворечивых

и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи	письменных и устных текстов учебной и научной тематики реферативного характера
ОК-8: Способность к самоорганизации и самообразованию	приобретать новые знания и умения; системно анализировать, обобщать информацию, формулировать цели и самостоятельно находить пути их достижения при решении профессиональных задач;	приобретения новых знаний и умений.
ОПК-5. Способность использовать нормативные правовые акты в профессиональной деятельности	применять правовые акты в профессиональной деятельности	работы с нормативными и методическими документами
ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	определять информационные ресурсы, подлежащие защите, угрозы безопасности информации	классификации информации ограниченного доступа
ПК-1. Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.	устанавливать технические средства защиты информации; грамотно эксплуатировать средства в соответствии с их технико-	конфигурации средств защиты в соответствии с требованиями документов по обеспечению информационной

	эксплуатационной документацией	безопасности на предприятии
ПК-2. Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.	использовать программные и аппаратные средства персонального компьютера	правилами использования программных и аппаратных средств персонального компьютера
ПК-3. Способность администрировать подсистемы информационной безопасности объекта защиты.	производить модернизацию подсистем безопасности объекта защиты в соответствии с руководящими документами	администрирования подсистем безопасности объекта защиты
ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.	формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	реализации политики безопасности на объекте практики
ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	осуществлять правовую оценку объекта информатизации; применять нормативные правовые акты и нормативные методические документы в области информационной безопасности; производить анализ информационной безопасности объекта	применения правовых актов и нормативных методических документов в области информационной безопасности
ПК-6. Способность принимать участие в организации и	использовать методику	анализа работоспособности

проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	контрольных проверок работоспособности и эффективности программных и программно-аппаратных средств защиты информации	и эффективности программных и программно-аппаратных средств защиты информации
ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	анализа исходных данных при проектировании подсистем и средств обеспечения информационной безопасности
ПК-8. Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	оформлять рабочую документацию с учетом действующих нормативных и методических документов	оформления рабочей документации с учетом действующих нормативных и методических документов
ПК-9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.	грамотно применять правовые документы для организации информационной безопасности на предприятии	проведения и обобщения результатов анализа информации, полученной из различных официальных документов и научной литературы
ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности	мониторинга и аудита, выявления угроз информационной безопасности информационных систем

	информационных систем	
ПК-11. Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	проводить эксперименты по заданной методике, обработку результатов	проведения экспериментов и обработки результатов
ПК-12. Способность принимать участие в проведении экспериментальных исследований системы защиты информации	принимать участие в проведении экспериментальных исследований системы защиты информации	проведения обследования объекта защиты информации на основании эксперимента
ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности	организации мер по обеспечению информационной безопасности
ПК-14. Способность организовать работу малого коллектива исполнителей в профессиональной деятельности	организовать работу в группе по обеспечению информационной безопасности информационной системы	применения профессиональной терминологии по информационной безопасности
ПК-15. Способность организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.	работы с нормативными правовыми актами
ПСК-1. Способность учитывать и использовать особенности информационных технологий, применяемых в	разрабатывать предложения по совершенствованию системы управления	конфигурирования параметров системы защиты информации

автоматизированных системах, при организации защиты обрабатываемой в них информации	защиты информации автоматизированных систем.	автоматизированных систем.
ПСК-2. Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	администрировать подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	конфигурирования параметров системы защиты информации автоматизированных систем.
ПСК-3. Способность планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	анализировать программные и аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах	подготовки документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации
ПСК-4. Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	разрабатывать программные и аппаратные средства обеспечения информационной безопасности.	проектирования и реализации программных средств для обеспечения информационной безопасности

3. Место практики в структуре образовательной программы

Преддипломная практика является составной частью ОПОП ВО – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем» и в полном объеме относится к вариативной части этой программы.

Преддипломная практика является обязательным этапом обучения бакалавра по направлению подготовки 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем» 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 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем».

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 отчетности по практике</i>
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 актов предприятия/организации	Отчет по 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиля «Безопасность автоматизированных систем».

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 информационной безопасности защищенных автоматизированных систем управления	Ставрополь : СКФУ, 2017. - 86 с.	https://biblioclub.ru/index.php?page=book_red&id=467139&sr=1
4.	Аверченков, В.И.	Служба защиты информации:	Москва : Издательство	https://biblioclub.ru/index.p

		организация и управление	«Флинта», 2016. - 186 с. ISBN 978-5-9765-1271-9	hp?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., Гульятеева 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, А.В. Пролетарский, Е.В. Смирнова, А.М. Суоров	Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.	http://biblioclub.ru/index.php?page=book&id=428820
11.	Мэйволд Э.	Безопасность сетей	Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.	http://biblioclub.ru/index.php?page=book&id=429035

Дополнительная учебная литература				
<i>а) Дополнительная учебная литература</i>				
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&id=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&id=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&id=429834
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. – Ростов-на-Дону ; Таганрог : Издательство	http://biblioclub.ru/index.php?page=book&id=561238

			Южного федерального университета, 2018. – 202	
Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ				
<ol style="list-style-type: none"> 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				
<ol style="list-style-type: none"> 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				
<ol style="list-style-type: none"> 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. 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.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. Перечень лицензионного программного обеспечения

- 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 занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 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.ura.it.ru).

Перечень учебно-наглядных пособий:

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

Лист актуализации рабочей программы преддипломной практики

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от « 22 » сентября 2020 г. № 2

Зав. кафедрой В.С. Тангев В.С.

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от « 22 » мая 2021 г. № 10

Зав. кафедрой В.С. Тангев В.С.

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от « _____ » _____ 20__ г. № _____

Зав. кафедрой _____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от « _____ » _____ 20__ г. № _____

Зав. кафедрой _____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от « _____ » _____ 20__ г. № _____

Зав. кафедрой _____