Минобрнауки России
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Сыктывкарский государственный университет имени Питирима Сорокина»
(ФГБОУ ВО «СГУ им. Питирима Сорокина»)

УТВЕРЖДАЮ
И.о. ректора
_____ Н.А. Михальченкова
«1» июня 2016 г.

ПРОГРАММА ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Направление подготовки
10.03.01 (090900) Информационная безопасность

Квалификация (степень) выпускника
Бакалавр

Сыктывкар 2016

1. Вид практики: (тип), способы и формы проведения практики.

Вид практики: преддипломная.

Способы проведения практики: стационарная.

Тип практики: практика по получению профессиональных умений и опыта профессиональной деятельности.

Преддипломная практика по получению профессиональных умений и опыта профессиональной деятельности проводится в 8 семестре в объеме 216 часов, продолжительностью 4 недели.

2. Цель преддипломной практики по получению профессиональных умений и опыта профессиональной деятельности и планируемые результаты практики.

Целью преддипломной практики является:

- закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин профессионального цикла базовой и вариативной частей, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника;
- изучение информационной структуры предприятия, как объекта информатизации;
- изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;
- формирование навыков самостоятельного решения поставленных производственных задач;
- выбор темы выпускной квалификационной работы и ее выполнение.

Задачи преддипломной практики

- закрепление и расширение теоретических и практических знаний;
- развитие профессиональных навыков и навыков деловой коммуникации;
- сбор необходимых материалов для написания отчета по практике;
- проведение анализа и обобщения результаты собственных исследований;
- получение практических данных, для написания выпускной квалификационной работы, приобретения навыков их обработки.

Данные задачи преддипломной практики, соотносятся со следующими **видами** и **задачами** профессиональной деятельности:

эксплуатационная деятельность:

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;

проектно-технологическая деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

проведение проектных расчетов элементов систем обеспечения информационной безопасности;

участие в разработке технологической и эксплуатационной документации;

проведение предварительного технико-экономического обоснования проектных расчетов;

экспериментально-исследовательская деятельность:

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;

организационно-управленческая деятельность:

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.

ПАСПОРТ КОМПЕТЕНЦИЙ

Код компетенции	*КОД контролируемой компетенции/или ее части/ формулировка компетенции*	*Перечень планируемых результатов*
ОК	способностью к кооперации с коллегами, работе в коллективе (ОК-5);	*Знать: должностные обязанности сотрудников в области защиты информации.* *Уметь:* *работать в команде, распределять обязанности по выполнению работ.* *Владеть: навыками командной работы, способностью выражать свои мысли и мнения в деловой форме общения.*
ОК	- способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК-6);	*Знать: основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ;* *основные понятия и методы в области управленческой деятельности.* *Уметь: опознавать нестандартные ситуации, использовать в практической деятельности правовые знания; анализировать основные правовые акты и осуществлять правовую оценку информации, нести персональную ответственность за нарушения нормативно-правовых требований, предпринимать необходимые меры по восстановлению нарушенных прав.* *Владеть: навыками принятия решений, навыками дискуссии по профессиональной тематике*
ОК	- способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к	*Знать: место своей будущей профессии в обществе.* *Уметь: находить управленческие*

	выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-7);	*решения в профессиональной деятельности.* *Владеть: теоретическими и практическими знаниями в области профессиональной деятельности.*
ОК	- способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления (ОК-8);	*Знать: методы выбора направления и проведения научного исследования; порядок оформления и представления результатов научной работы;* *Уметь: определять цель и задачи предметной области, делать обоснованные выводы.* *Владеть: методами анализа информационных источников в области оптимизации задач.*
ОК	- способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-9);	*Знать: грамматические нормы русского языка и стилистических оборотов речи.* *Уметь: делать четкие, обоснованные выводы, быстро передавать и воспринимать определенное содержание информации.* *Владеть: умением готовить и представлять материалы в виде отчетов, публикаций, презентаций; навыками дискуссии по профессиональной тематике.*
ОК	- способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства (ОК-11);	*Знать: формы и методы профессионального развития своей индивидуальности.* *Уметь: усваивать определенные совокупности знаний, умений, навыков и приобретать профессионально-значимые качества.* *Владеть: навыками организации системного сбора, обработки и представления информации.*
ОК	- способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков (ОК-12);	*Знать: систему критериев коллективной оценки публичных выступлений.* *Уметь: демонстрировать способность участвовать в дискуссиях и отстаивать свою точку зрения опираясь на базу знаний.* *Владеть навыками самоконтроля и персональной ответственности.*
ПК	- способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1);	*Знать*: *основные естественнонаучные законы.* *Уметь: использовать знания об основных естественнонаучных закономерностях в решении задач анализа и разработки систем информационной безопасности, применять математические методы в*

		процессах диагностики состояния сложных организационно-технологических систем, правильно производить вычисления. *Владеть: приёмами работы с аппаратурой для проведения физических исследований, математическими методами для решения задач производственного характера.*
ПК	- способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-2);	*Знать: виды источников информации, средства информационных технологий.* *Уметь: пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.* *Владеть: основами автоматизации решения инженерных задач вычислительного характера; умением анализировать и систематизировать результаты исследований.*
ПК	- способностью использовать нормативные правовые документы в своей профессиональной деятельности (ПК-3);	*Знать: требования нормативных правовых документов в своей профессиональной области.* *Уметь: использовать в практической деятельности правовые знания; анализировать основные правовые акты и осуществлять правовую оценку информации* *Владеть: навыками использования нормативной базы РФ*
ПК	- способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4);	*Знать: меры по обеспечению информационной безопасности; принципы организации информационных систем в соответствии с требованиями по защите информации;* *Уметь:* формулировать *политику безопасности, осуществлять меры противодействия нарушениям, анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации; анализировать и оценивать степень риска проявления факторов опасности системы.* *Владеть: навыками организации мероприятий по защите информации на объекте информатизации; навыками принятия экономических решений.*
ПК	- способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта	*Знать: организационную структуру объекта защиты, факторы, воздействующие на объект защиты информации, структуру систем документационного обеспечения;* *Уметь:* формулировать *политику*

	защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-5);	*безопасности, осуществлять меры противодействия нарушениям, анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации; анализировать и оценивать степень риска проявления факторов опасности системы.* *Владеть: навыками организации мероприятий по защите информации на объекте информатизации.*
ПК	- способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-8);	*Знать: виды информации и ее носителей, классификацию угроз информации, уязвимости информации, структуру и содержание информационных процессов предприятия, технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.* *Уметь: анализировать и оценивать угрозы информационной безопасности объекта; разрабатывать нормативно-методические документы по защите информации.* *Владеть: методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы.*
ПК	- способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-9);	*Знать: функции подсистем управления информационной безопасностью на предприятии.* *Уметь: использовать различные программные и аппаратные средства защиты; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.* *Владеть: навыками проведения оценки защищенности помещений от утечки информации, навыками разработки мероприятий по защите информации от утечки*
ПК	способностью администрировать подсистемы информационной безопасности объекта (ПК-10);	*Знать: аппаратные средства вычислительной техники, операционные системы, основы администрирования автоматизированных систем.* *Уметь: проводить анализ сетевого трафика, применять программно-аппаратные средства защиты информации.* *Владеть: навыками работы администратора компьютерных сетей.*

ПК	- способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-11);	*Знать: аппаратные средства вычислительной техники; операционные системы, основы администрирования вычислительных сетей; системы управления базами данных.* *Уметь: настраивать и обслуживать средства защиты информации.* *Владеть: навыками работы использования технических средств идентификации и проверки подлинности пользователей компьютерных систем, навыками проведения оценки защищенности помещений от утечки.*
ПК	- способностью участвовать в разработке подсистемы управления информационной безопасностью (ПК-12);	*Знать: современные средства разработки и анализа программного обеспечения, принципы построения информационных систем;* *Уметь: применять программные средства обеспечения защиты информации.* *Владеть: навыками работы с информационными системами.*
ПК	- способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности (ПК-13);	*Знать: методы оценки угроз и степени риска.* *Уметь: проводить технико-экономический анализ решений по обеспечению информационной безопасности.* *Владеть: технологией проектирования информационных систем защиты, методами оценки уровня информационной безопасности.*
ПК	- способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности (ПК-14);	*Знать: структуру систем документационного обеспечения;* *Уметь: оформлять техническую и методическую документацию в области информационной безопасности.* *Владеть: навыками составления документов с применением современного программного обеспечения.*
ПК	- способностью применять программные средства системного, прикладного и специального назначения (ПК-15);	*Знать: современные средства разработки и анализа программного обеспечения, операционные системы, правовые нормы по вопросам сертификации и лицензирования в области защиты информации.* *Уметь: применять программные средства системного, прикладного и специального назначения.* *Владеть: навыками защиты от разрушающих программных воздействий;*

		навыками рационального выбора средств и методов защиты информации объектов информатизации.
ПК	- способностью использовать инструментальные средства и системы программирования для решения профессиональных задач (ПК-16);	*Знать: методы программирования и методы разработки эффективных алгоритмов решения прикладных задач.* *Уметь: использовать инструментальные средства и системы программирования.* *Владеть: навыками разработки, документирования, тестирования и отладки программ; навыками программирования для решения практических задач.*
ПК	- способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности (ПК-19);	*Знать: методики проведения аудита в области информационной безопасности.* *Уметь: применять методики проведения аудита в области информационной безопасности.* *Владеть: навыками организации системного сбора, обработки и представления информации.*
ПК	- способностью применять методы анализа изучаемых явлений, процессов и проектных решений (ПК-20);	*Знать: методы получения и сбора значимой информации.* *Уметь: делать выводы на основании проведенного анализа.* *Владеть: навыками разработки систем мониторинга информационной безопасности; навыками применения различных методов и мер обеспечения информационной безопасности.*
ПК	- способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности (ПК-24);	*Знать: виды источников и носителей информации.* *Уметь: обобщать большие объемы информации, полученные в результате изучения различных источников.* *Владеть: навыками организации системного сбора, обработки и представления информации.*
ПК	- способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-28);	*Знать: сравнительные характеристики профессиональной деятельности организаций различных форм собственности.* *Уметь: обобщать опыт работы других организаций, изученный по открытым источникам информации.* *Владеть: навыками исследования организационной среды предприятия.*
ПК	- способностью участвовать в работах по реализации политики информационной безопасности (ПК-29);	*Знать: возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, специфику деятельности объекта защиты, методы документирования информации.*

		Уметь: определять функции взаимодействия структурных подразделений, разрабатывать политику информационной безопасности объекта защиты. *Владеть: навыками планирования и организации системы защиты информации.*
ПК	- способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации (ПК-32);	*Знать: требования по охране труда и технике безопасности.* *Уметь: анализировать и оценивать степень риска проявления факторов опасности системы "человек - среда обитания", осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности.* *Владеть: инженерными решениями по обеспечению безопасных и здоровых условий труда в современных производствах.*

3. Место преддипломной практики по получению профессиональных умений и опыта профессиональной деятельности в структуре ООП ВО.

Преддипломная практика является составной частью учебного процесса и обязательна для каждого студента. Данный вид практики входит в раздел «Б.5. Учебная иПреддипломная практики» ФГОС-3 по направлению подготовки ВО шифр – 090900 «Информационная безопасность».

Преддипломная практика является обязательным этапом обучения бакалавра по направлению «Информационная безопасность» и предусматривается учебным планом соответствующих подразделений вузов; ей предшествуют курсы «Математики», «Информатики», «Экономики», «Иностранный язык», «Структуры и основы деятельности предприятий различных форм собственности», «Физики», «Концепции современного естествознания», «Математическая логика и теория алгоритмов», «Безопасность жизнедеятельности», «Документоведение», «Основы программирования», «Основы информационных технологий», «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Языки программирования», «Электротехника», «Операционные системы и оболочки», «Операционная система Linux», «История российских спецслужб», «Математические основы криптологии», «Информационные технологии», «Информационная безопасность автоматизированных систем», «Инженерно-техническая защита информации», «Электрорадиоизмерения», «Основы радиотехники», «Экономика защиты информации», «Правоведение», «Управление рисками», «Базы данных», «Web-программирование», «Сети и системы передачи информации», «Безопасность вычислительных сетей», «Физика волновых процессов», «Электроника и схемотехника», «Теория информации», «Информационная безопасность предприятия», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности» предполагающих проведение лекционных и семинарских занятий с обязательным итоговым контролем в форме зачетов и экзаменов.

Требования к входным знаниям, умениям и готовности студентов, приобретенных в результате освоения предшествующих частей ООП: студент должен

знать:

основные понятия экономической и финансовой деятельности отрасли и ее структурных подразделений, основные понятия и методы математического анализа, основные понятия, законы и модели электричества и магнетизма, основные понятия и методы математической логики и теории алгоритмов, теории информации и кодирования, основные понятия, законы и модели теории колебаний и волн, оптики, квантовой физики, физики твердого тела, особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности, основные понятия информатики, место и роль информационной безопасности в системе национальной безопасности РФ, методы программирования, аппаратные средства вычислительной техники, операционные системы персональных ЭВМ, принципы построения информационных систем, системы управления базами данных, структуру систем документационного обеспечения, технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации, принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации, принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы протекающие в них, основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти Российской Федерации; характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности Российской Федерации, основные понятия и методы в области управленческой деятельности;

быть готовым к:

оценке эффективности управленческих решений, письменному изложению собственной точки зрения, ведению дискуссий и полемике, владению иностранным языком, в объеме, необходимом для получения информации по профессиональной тематике, использованию программных и аппаратных средств персонального компьютера, поиску информации в глобальной информационной сети Интернет и работы с офисными приложениями, выбору необходимых инструментальных средств для разработки программ в различных операционных системах, составлению, тестированию и отлаживанию программ на языках высокого уровня, оценке угроз информационной безопасности объекта, использованию профессиональной терминологии, выявлению и уничтожению компьютерных вирусов, формулировать и настраивать политику безопасности распространенных операционных систем, осуществлению мер противодействия нарушениям информационной безопасности с использованием аппаратных и программных средств защиты, анализу и оценке угрозы информационной безопасности объекта, использованию нормативных документов по защите информации, выполнению требований по охране труда и технике безопасности в конкретной сфере деятельности, применять отечественные и зарубежные стандарты в области безопасности, выявлению угроз безопасности АС, использованию методов технической защиты информации, проведению расчетов и инструментального контроля показателей технической защиты информации, анализу сетевого трафика, результатов работы средств обнаружения вторжений, работе с нормативными правовыми актами, работе по выявлению угрозы безопасности автоматизированным системам, организации и обеспечению режима секретности, использованию методов формирования требований по защите информации, использованию правовых знаний, анализу и составлению основных правовых актов и осуществлению правовой оценки информации, предпринимать необходимые меры по восстановлению нарушенных прав, анализу и оценке социальной информации, оценке эффективности управленческих решений и анализу экономических показателей деятельности подразделения.

4. Объём преддипломной практики по получению профессиональных умений и опыта профессиональной деятельности и ее продолжительность

Общая трудоемкость преддипломной практики составляет 6 зачетных единиц, 216 часов. Преддипломная практика проходит в 8 семестре, в течение 4 недель.

Преддипломная практика проходит на базе организаций или предприятий, использующих в своей деятельности различные системы защиты информации, предприятий

оказывающих услуги в области защиты информации и предприятий, проводящих работы по защите информации в своей организации и за ее пределами, а так же организаций, проводящих исследования и расследования в области обеспечения информационной безопасности. Базы практики находятся как в Республике Коми, так и за ее пределами.

Преддипломная практика, организуемая на базе сторонних организаций, осуществляется на основе договоров между Университетом и соответствующими предприятиями, организациями и учреждениями. В договоре университет и предприятие (организация и учреждение) оговаривают все вопросы, касающиеся проведения практики, в том числе и по назначению двух руководителей практики: от Университета и предприятия или организации или учреждения.

Руководство практикой от Университета осуществляют преподаватели кафедры информационной безопасности; от организации – специалист в области информационной безопасности или руководитель подразделения организации.

Студенты, заключившие с организациями индивидуальный договор (контракт) о целевой контрактной подготовке, преддипломную практику, как правило, проходят в этих организациях.

5. Содержание преддипломной практики по получению профессиональных умений и опыта профессиональной деятельности

№ п/п	Этапы практики	Содержание деятельности	Формы текущего контроля (отчетности)
1	Ознакомительно-подготовительный	- Общее собрание обучающихся по вопросам организации учебной практики; - инструктаж по технике безопасности; - ознакомление их с программойпреддипломной практики, целями и задачами практики; - ознакомление с организацией прохождения практики; - ознакомление с тематикой индивидуальных заданий; - ознакомление обучающегося с формой и видом отчетности; - ознакомление с порядком защиты отчета по преддипломной практике и требованиями к оформлению отчета по учебной практике; - подбор материала для прохождения практики.	Распоряжение о допуске к прохождению практики. Присутствие на установочной конференции.
2	Деятельностный	Ознакомление с деятельностью предприятия. Определение методов и средств защиты информации, используемых на предприятии. Выполнение практических заданий. Сбор материалов для отчетной документации.	Требования. Рекомендации. Пошаговый анализ выполнения практических заданий. Оформление отчетной документации. Согласование отчета с руководителем практики от предприятия.
3	Оценочно-результативный	Систематизация и анализ выполненных заданий.	Анализ отчетной документации за период практики.

		Оформление отчетной документации.	Отчет о прохождении практики на итоговой конференции. Оценка работы.

Преддипломная практика предполагает: производственный инструктаж, в т.ч. инструктаж по технике безопасности; выполнение производственных заданий; сбор, обработка и систематизация фактического и литературного материала; наблюдения; измерения и другие, выполняемые обучающимся самостоятельно виды работ.

На каждом рабочем месте проводится инструктаж по ТБ. Студент должен усвоить полученный материал и расписаться в соответствующем журнале. Находясь на практике, студент подчиняется правилам внутреннего распорядка, установленным для работников предприятия.

В начале практики руководитель от предприятия совместно со студентом составляют план прохождения практики с учетом тематики примерных практических заданий рекомендованных данной программой практики, профилем и технической оснащенностью данного предприятия. План прохождения практики согласовывается с руководителем практики от Университета.

Преддипломная практика предполагает непосредственное участие студентов в деятельности предприятия.

Студент обязан добросовестно и качественно выполнять порученную ему работу.

Методическое и консультационное обеспечение осуществляет руководитель практики от Университета или заведующий кафедрой информационной безопасности.

На конечном этапе практики студент составляет отчет о прохождении практики и согласовывает его с руководителем практики от организации. Отчет подписывается студентом и руководителем практики от предприятия и Университета. (см.прил. 1).

6. Формы отчетности по преддипломной практике по получению профессиональных умений и опыта профессиональной деятельности

Формы отчетности по практике	• *«Удостоверение» о направлении на практику, завизированное в организации;* • *дневник преддипломной практики, заполненный в соответствии с установленными требованиями;* • *лист экспертной оценки, подписанный руководителем практики от организации, заверенный печатью организации (предприятия) (см. прил. 2);* • *отчет о практике, по содержанию включающий в себя результаты выполненных работ.*
*Сроки получения допуска к прохождению практики (*Инструктаж по технике безопасности и пожарной безопасности обучающиеся получают от руководителя практики и расписываются в журнале*);*	*За месяц до начала практики*
Сроки проведения установочной конференции по практике;	*За месяц до начала практики*
Сроки сдачи документов по практике для проверки в институт;	*В течение недели после окончания практики*
Сроки проведения итоговой конференции по практике.	*В течение месяца после окончания практики. Сроки итоговой конференции устанавливаются распоряжением директора института.*
Форма итогового контроля по практике.	*Защита итогового отчета о прохождении преддипломной практики на итоговой*

	конференции.

Отчет оформляется с помощью печатающих устройств на одной стороне листа бумаги формата А4. Размер шрифта 12-14 через 1-1,5 интервала. При написании текста следует оставлять поля слева - 30 мм, справа - 10 мм, сверху и снизу - 20 мм. Все страницы должны иметь сквозную нумерацию: первой страницей является титульный лист. На титульном листе номер не ставится. Номер страницы проставляется в низу по центру.

Отчет о практике является обязательным документом студентов-практикантов. По форме он должен включать титульный лист (см. прил. 1) и текст отчета (см. прил. 3). Отчет обязательно должен содержать не только информацию о выполнении заданий программы практики, но и анализ этой информации, выводы и рекомендации, разработанные студентом самостоятельно. Оформленный итоговый отчет должен быть сброшюрован в папку со скоросшивателем. Титульный лист должен быть подписан руководителями практики и студентом-практикантом.

Отчёт может содержать приложения:
- материалы, собранные студентом в период прохождения практики (копии нормативно правовых и организационных документов, а также те документы, в составлении которых студент, принимал непосредственное участие в объёме, предусмотренном заданием);
- схемы, таблицы, аналитические расчёты, статистические данные, иллюстрации и т.п.

Отчет готовится в течение всей практики и проверяется преподавателем-руководителем практики до защиты практики. Оформленный отчет о практике, подлежит обязательной защите студентом в установленные сроки.

По окончании преддипломной практики руководитель практики от предприятия дает отзыв о прохождении практики студентом в **листе экспертной оценки.** В отзыве должна быть дана характеристика студента со стороны овладения им знаний, умений и навыков для решения производственных задач в области обеспечения информационной безопасности, произведена оценка уровня сформированности компетенций в различных видах профессиональной деятельности и отмечены достоинства и недостатки в его профессиональной подготовке.

Аттестация по итогам преддипломной практики проводится на основании материалов отчета о практике, дневника преддипломной практики и листа экспертной оценки, оформленных в соответствии с установленными требованиями.

Прием зачета по практике производит комиссия. В состав комиссии входят заведующий кафедрой, руководитель практики от Университета, руководитель практики от предприятия и другие преподаватели, назначенные распоряжением директора института.

По итогам аттестации выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно).

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по преддипломной практике по получению профессиональных умений и опыта профессиональной деятельности

7.1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные практические задания:

1. ознакомиться с историей, традициями и сферами деятельности предприятия согласно уставу или положению о предприятии и пройти инструктаж по технике безопасности на рабочем месте;
2. описать организационную структуру предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие;
3. определить виды информации ограниченного доступа, обрабатываемые предприятием;

4. ознакомиться с формами организации производственного процесса и его технологическим обеспечением;
5. выявить угрозы безопасности предприятия;
6. проанализировать организационно-правовую документацию предприятия в области обеспечения информационной безопасности;
7. изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации;
8. изучить методы и средства защиты информации, применяемые на предприятии;
9. изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта;
10. разработать модель угроз для конкретной информационной системы предприятия;
11. изучить основные обязанности должностных лиц в области защиты информации;
12. проанализировать методы контроля в области защиты информации, используемые в организации;
13. разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия;
14. предложить перечень мероприятий по улучшению системы защиты информации на предприятии.
15. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности;
16. провести анализ безопасности программных продуктов, используемых на предприятии;
17. изучить возможные методы прогнозирования появления уязвимостей в программном коде;
18. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД;
19. изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации;
20. спроектировать систему ИТЗИ кабинета руководителя организации или выделенного помещения;
21. спроектировать систему физической защиты информации;
22. разработать политику информационной безопасности предприятия;
23. проанализировать систему компьютерной безопасности предприятия;
24. изучить систему контроля и управления доступом предприятия;
25. изучить систему защиты персональных данных в организации;
26. изучить виды правонарушений при совершении компьютерных преступлений;
27. провести анализ рисков информационной безопасности;
28. разработать программное решение для обеспечения информационной безопасности;
29. провести исследования вредоносного кода;
30. исследовать проблемы безопасности при использовании мобильных устройств;
31. изучить обеспечение информационной безопасности при использовании СЭД;
32. исследовать криптографические методы защиты информации;
33. исследовать способы защиты мультисервисных сетей;
34. подготовка отчета о прохождении преддипломной практики;
35. защита отчета.

7.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Перечень Компетенции	*Этапы формирования компетенций*
ОК-5	1. ознакомиться с историей, традициями и сферами деятельности предприятия согласно уставу или положению о предприятии и пройти инструктаж по технике безопасности на рабочем месте;

	2. описать организационную структуру предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие; 4. ознакомиться с формами организации производственного процесса и его технологическим обеспечением;
ОК-6	10. разработать модель угроз для конкретной информационной системы предприятия; 12. проанализировать методы контроля в области защиты информации, используемые в организации; 13. разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия; 20. спроектировать систему ИТЗИ кабинета руководителя организации или выделенного помещения; 21. спроектировать систему физической защиты информации; 22. разработать политику информационной безопасности предприятия; 27.провести анализ рисков информационной безопасности;
ОК-7	3. определить виды информации ограниченного доступа, обрабатываемые предприятием; 5. выявить угрозы безопасности предприятия; 8. изучить методы и средства защиты информации, применяемые на предприятии; 14. предложить перечень мероприятий по улучшению системы защиты информации на предприятии.
ОК-8	18. проанализировать организационно-правовую документацию предприятия в области обеспечения информационной безопасности; 19. проанализировать методы контроля в области защиты информации, используемые в организации; 20. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности; 21. провести анализ безопасности программных продуктов, используемых на предприятии; 22. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД; 23. проанализировать систему компьютерной безопасности предприятия;
ОК-9	34. подготовка отчета о прохождении производственной практики. 35. защита отчета.
ОК-11	3. определить виды информации ограниченного доступа, обрабатываемые предприятием; 5.выявить угрозы безопасности предприятия; 8.изучить методы и средства защиты информации, применяемые на предприятии; 10.разработать модель угроз для конкретной информационной системы предприятия; 11.изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта; 13.разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия; 17.изучить возможные методы прогнозирования появления уязвимостей в программном коде;

	19.изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации; 20.спроектировать систему ИТЗИ кабинета руководителя организации или выделенного помещения; 21. спроектировать систему физической защиты информации; 24.изучить систему контроля и управления доступом предприятия; 25.изучить систему защиты персональных данных в организации; 26.изучить виды правонарушений при совершении компьютерных преступлений; 28.разработать программное решение для обеспечения информационной безопасности;
ОК-12	11. изучить основные обязанности должностных лиц в области защиты информации; 15. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности;
ПК-1	9.изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта; 15.оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности; 16.провести анализ безопасности программных продуктов, используемых на предприятии; 17.изучить возможные методы прогнозирования появления уязвимостей в программном коде; 28. разработать программное решение для обеспечения информационной безопасности; 29. провести исследования вредоносного кода; 30. исследовать проблемы безопасности при использовании мобильных устройств; 32. исследовать криптографические методы защиты информации; 33. исследовать способы защиты мультисервисных сетей;
ПК-2	9.изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта; 15.оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности; 16.провести анализ безопасности программных продуктов, используемых на предприятии; 17.изучить возможные методы прогнозирования появления уязвимостей в программном коде; 18.произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД; 28. разработать программное решение для обеспечения информационной безопасности; 29. провести исследования вредоносного кода; 30. исследовать проблемы безопасности при использовании мобильных устройств; 31. изучить обеспечение информационной безопасности при использовании СЭД; 32. исследовать криптографические методы защиты информации;

	33. исследовать способы защиты мультисервисных сетей;
ПК-3	1. ознакомиться с историей, традициями и сферами деятельности предприятия согласно уставу или положению о предприятии и пройти инструктаж по технике безопасности на рабочем месте; 2. описать организационную структуру предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие; 3. определить виды информации ограниченного доступа, обрабатываемые предприятием; 6. проанализировать организационно-правовую документацию предприятия в области обеспечения информационной безопасности; 8. изучить методы и средства защиты информации, применяемые на предприятии; 11. изучить основные обязанности должностных лиц в области защиты информации; 22. разработать политику информационной безопасности предприятия; 25. изучить систему защиты персональных данных в организации; 26. изучить виды правонарушений при совершении компьютерных преступлений;
ПК-4	5. выявить угрозы безопасности предприятия; 6. проанализировать организационно-правовую документацию предприятия в области обеспечения информационной безопасности; 7. изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации; 8. изучить методы и средства защиты информации, применяемые на предприятии; 9. изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта; 14. предложить перечень мероприятий по улучшению системы защиты информации на предприятии. 15. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности; 24. изучить систему контроля и управления доступом предприятия; 29.провести исследования вредоносного кода; 30.исследовать проблемы безопасности при использовании мобильных устройств; 31.изучить обеспечение информационной безопасности при использовании СЭД; 32. исследовать криптографические методы защиты информации; 33.исследовать способы защиты мультисервисных сетей;
ПК-5	5. выявить угрозы безопасности предприятия; 10. разработать модель угроз для конкретной информационной системы предприятия; 13. разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия; 15. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности; 16. провести анализ безопасности программных продуктов, используемых на предприятии; 17. изучить возможные методы прогнозирования появления уязвимостей в программном коде; 18. произвести анализ безопасности используемых на предприятии СУБД,

	предложить методики улучшения эффективности безопасности СУБД; 19. изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации; 20. спроектировать систему ИТЗИ кабинета руководителя организации или выделенного помещения; 22. спроектировать систему физической защиты информации; 23. разработать политику информационной безопасности предприятия; 24. проанализировать систему компьютерной безопасности предприятия; 25. изучить систему контроля и управления доступом предприятия; 26. изучить систему защиты персональных данных в организации; 27.провести анализ рисков информационной безопасности; 29.провести исследования вредоносного кода; 30.исследовать проблемы безопасности при использовании мобильных устройств; 31.изучить обеспечение информационной безопасности при использовании СЭД; 32. исследовать криптографические методы защиты информации; 33.исследовать способы защиты мультисервисных сетей;
ПК-8	3. определить виды информации ограниченного доступа, обрабатываемые предприятием; 4. ознакомиться с формами организации производственного процесса и его технологическим обеспечением; 5. выявить угрозы безопасности предприятия; 6. проанализировать организационно-правовую документацию предприятия в области обеспечения информационной безопасности; 8. изучить методы и средства защиты информации, применяемые на предприятии; 10. разработать модель угроз для конкретной информационной системы предприятия; 15. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности; 16. провести анализ безопасности программных продуктов, используемых на предприятии; 17. изучить возможные методы прогнозирования появления уязвимостей в программном коде; 18. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД; 22.разработать политику информационной безопасности предприятия; 27.провести анализ рисков информационной безопасности; 29.провести исследования вредоносного кода; 30.исследовать проблемы безопасности при использовании мобильных устройств; 31.изучить обеспечение информационной безопасности при использовании СЭД; 32. исследовать криптографические методы защиты информации; 33.исследовать способы защиты мультисервисных сетей;
ПК-9	7. изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации; 9. изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта; 16. провести анализ безопасности программных продуктов,

	используемых на предприятии; 17. изучить возможные методы прогнозирования появления уязвимостей в программном коде; 18. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД; 20. спроектировать систему ИТЗИ кабинета руководителя организации или выделенного помещения; 21. спроектировать систему физической защиты информации; 23. проанализировать систему компьютерной безопасности предприятия; 24. изучить систему контроля и управления доступом предприятия; 25. изучить систему защиты персональных данных в организации; 29. провести исследования вредоносного кода; 30. исследовать проблемы безопасности при использовании мобильных устройств; 31. изучить обеспечение информационной безопасности при использовании СЭД; 32. исследовать криптографические методы защиты информации; 33. исследовать способы защиты мультисервисных сетей;
ПК-10	9. изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта; 16. провести анализ безопасности программных продуктов, используемых на предприятии; 17. изучить возможные методы прогнозирования появления уязвимостей в программном коде; 18. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД; 20. спроектировать систему ИТЗИ кабинета руководителя организации или выделенного помещения; 21. спроектировать систему физической защиты информации; 23. проанализировать систему компьютерной безопасности предприятия; 24. изучить систему контроля и управления доступом предприятия; 25. изучить систему защиты персональных данных в организации; 28. разработать программное решение для обеспечения информационной безопасности; 31. изучить обеспечение информационной безопасности при использовании СЭД;
ПК-11	7. изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации; 9. изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта; 16. провести анализ безопасности программных продуктов, используемых на предприятии; 17. изучить возможные методы прогнозирования появления уязвимостей в программном коде; 18. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД;

ПК-12	10. разработать модель угроз для конкретной информационной системы предприятия; 13. разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия; 15. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности; 20. спроектировать систему ИТЗИ кабинета руководителя организации или выделенного помещения; 22. разработать политику информационной безопасности предприятия; 28. разработать программное решение для обеспечения информационной безопасности;
ПК-13	8. изучить методы и средства защиты информации, применяемые на предприятии; 12. проанализировать методы контроля в области защиты информации, используемые в организации; 15. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности; 16. провести анализ безопасности программных продуктов, используемых на предприятии; 17. изучить возможные методы прогнозирования появления уязвимостей в программном коде; 18. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД; 19. изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации; 24. изучить систему контроля и управления доступом предприятия; 25. изучить систему защиты персональных данных в организации; 26. изучить виды правонарушений при совершении компьютерных преступлений;
ПК-14	10. разработать модель угроз для конкретной информационной системы предприятия; 13. разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия; 14. предложить перечень мероприятий по улучшению системы защиты информации на предприятии. 22. разработать политику информационной безопасности предприятия; 25. изучить систему защиты персональных данных в организации;
ПК-15	7. изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации; 9. изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта; 16. провести анализ безопасности программных продуктов, используемых на предприятии; 17. изучить возможные методы прогнозирования появления уязвимостей в программном коде; 18. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД; 23. проанализировать систему компьютерной безопасности предприятия; 28. разработать программное решение для обеспечения

	информационной безопасности; 29. провести исследования вредоносного кода; 30. исследовать проблемы безопасности при использовании мобильных устройств; 31. изучить обеспечение информационной безопасности при использовании СЭД; 32. исследовать криптографические методы защиты информации; 33. исследовать способы защиты мультисервисных сетей;
ПК-16	7. изучить особенности эксплуатации и состав технических, программных и аппаратных средств защиты информации; 9. изучить основные характеристики и возможности, используемых в подразделении технических, программных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта; 16. провести анализ безопасности программных продуктов, используемых на предприятии; 17. изучить возможные методы прогнозирования появления уязвимостей в программном коде; 18. произвести анализ безопасности используемых на предприятии СУБД, предложить методики улучшения эффективности безопасности СУБД; 23. проанализировать систему компьютерной безопасности предприятия; 28. разработать программное решение для обеспечения информационной безопасности; 29. провести исследования вредоносного кода;
ПК-19	1. ознакомиться с историей, традициями и сферами деятельности предприятия согласно уставу или положению о предприятии и пройти инструктаж по технике безопасности на рабочем месте; 2. описать организационную структуру предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие; 3. определить виды информации ограниченного доступа, обрабатываемые предприятием; 6. проанализировать организационно-правовую документацию предприятия в области обеспечения информационной безопасности; 8. изучить методы и средства защиты информации, применяемые на предприятии; 11. изучить основные обязанности должностных лиц в области защиты информации; 22. разработать политику информационной безопасности предприятия; 25. изучить систему защиты персональных данных в организации; 26. изучить виды правонарушений при совершении компьютерных преступлений;
ПК-20	8. изучить методы и средства защиты информации, применяемые на предприятии; 12. проанализировать методы контроля в области защиты информации, используемые в организации; 15. оценить информационные активы предприятия, степень их защищенности и меры, необходимые для обеспечения информационной безопасности; 16. провести анализ безопасности программных продуктов, используемых на предприятии; 17. изучить возможные методы прогнозирования появления уязвимостей в программном коде; 18. произвести анализ безопасности используемых на предприятии

	СУБД, предложить методики улучшения эффективности безопасности СУБД; 19. изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации; 24. изучить систему контроля и управления доступом предприятия; 25. изучить систему защиты персональных данных в организации; 26. изучить виды правонарушений при совершении компьютерных преступлений; 27. провести анализ рисков информационной безопасности;
ПК-24	1. ознакомиться с историей, традициями и сферами деятельности предприятия согласно уставу или положению о предприятии и пройти инструктаж по технике безопасности на рабочем месте; 2. описать организационную структуру предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие; 3. определить виды информации ограниченного доступа, обрабатываемые предприятием; 6. проанализировать организационно-правовую документацию предприятия в области обеспечения информационной безопасности; 8. изучить методы и средства защиты информации, применяемые на предприятии; 11. изучить основные обязанности должностных лиц в области защиты информации; 19. изучить организационно-технические мероприятия по закрытию выявленных технических каналов утечки информации; 24. изучить систему контроля и управления доступом предприятия; 25. изучить систему защиты персональных данных в организации; 26. изучить виды правонарушений при совершении компьютерных преступлений;
ПК-28	10. разработать модель угроз для конкретной информационной системы предприятия; 12. проанализировать методы контроля в области защиты информации, используемые в организации; 13. разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия; 14. предложить перечень мероприятий по улучшению системы защиты информации на предприятии. 27. провести анализ рисков информационной безопасности;
ПК-29	2.описать организационную структуру предприятия: схема, количество отделов и их название, их функции, подчиненность, взаимодействие; 3.определить виды информации ограниченного доступа, обрабатываемые предприятием; 5.выявить угрозы безопасности предприятия; 6.проанализировать организационно-правовую документацию предприятия в области обеспечения информационной безопасности; 8.изучить методы и средства защиты информации, применяемые на предприятии; 10.разработать модель угроз для конкретной информационной системы предприятия; 13.разработать перечень мероприятий по устранению выявленных недостатков в системе защиты информации предприятия; 22. разработать политику информационной безопасности предприятия;
ПК-32	1.ознакомиться с историей, традициями и сферами деятельности предприятия согласно уставу или положению о предприятии и пройти инструктаж по технике безопасности на рабочем месте;

7.3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Оценку уровня сформированности компетенций на различных этапах их формирования определяет руководитель практики от предприятия, путем проставления подписи в дневнике практики за каждое выполненное практическое задание. Наличие подписи руководителя практики за выполнение задания является показателем сформированности закрепленной компетенции на данном этапе формирования.

Каждое выполненное практическое задание оценивается «зачет/незачет» по следующим основным критериям:

1. Уровень выполнения задания: соответствует формированию закрепленной компетенции.
2. Полнота раскрытия темы задания, обоснованность выводов, предложений.

Так же итоговая оценка уровня сформированности компетенций в различных видах профессиональной деятельности дается руководителем практики от предприятия в **листе экспертной оценки.**

Аттестация по итогам преддипломной практики проводится на основании материалов отчета о практике, дневника преддипломной практики и листа экспертной оценки, оформленных в соответствии с установленными требованиями.

При получении «зачета» за выполнение практического задания, закрепленная в соответствии с таблицей компетенция считается частично сформированной.

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Прием зачета по практике производит комиссия. В состав комиссии входят заведующий кафедрой, руководитель практики от Университета, руководитель практики от предприятия и другие преподаватели, назначенные распоряжением директора института.

Оценка выполненной работы производится на основе ответов студента, отзыва руководителя практики от предприятия, зафиксированного в листе экспертной оценки, а так же содержания и качества оформления отчета.

Содержание отчета оценивается по следующим критериям:

1. Уровень выполнения задания соответствует формированию закрепленной компетенции.
2. Темы заданий раскрыты в полном объеме.
3. Приведены обоснованные выводы.
4. Представлены предложения.
5. Качество оформления отчета соответствует установленным требованиям.
6. Выражена степень самостоятельности в работе: индивидуальный стиль изложения, оригинальность представленных иллюстраций и других собранных материалов.
7. Используется научно-исследовательский подход, грамотность, стилистическая правильность текста.

Защита **итогового отчета о прохождении преддипломной практики** проводится в назначенное время и включает:

- предоставление «удостоверения», дневника практики, письменного отчета о прохождении практики, листа экспертной оценки.
- краткое сообщение студента о результатах преддипломной практики, проведенных исследованиях и конкретных предложениях (3-5 минут).
- вопросы к студенту и ответы на них (3-5 минут).

По итогам защиты отчета выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно).

Критерии оценки:

"Отлично" оценивается работа студента, выполнившего весь объем работы, определенной программой практики, проявившего теоретическую подготовку и умелое применение полученных знаний в ходе практики, оформившего отчет о практике в соответствии со всеми требованиями; уверенно владеющего материалом при устной защите и правильно отвечающего на вопросы.

"Хорошо" - оценивается работа студента, который полностью выполнил программу практики, проявил самостоятельность, интерес к профессиональной деятельности, однако, при оформлении отчета о практике и (или) при ответах на вопросы допустил недочеты;

"Удовлетворительно" - оценивается работа студента, который выполнил программу практики, но при этом не проявил самостоятельности, допустил небрежность в формулировании выводов в отчете практики, не показал интереса к выполнению заданий практики, небрежно оформил отчет о практике, несвоевременно представил отчетные документы, допускал существенные недочеты при ответах на вопросы.

"Неудовлетворительно" - оценивается работа студента, не выполнившего программу практики, непредставившего отчет о практике или представившего отчет о практике, выполненный на крайне низком уровне, систематически непосещавшего базу практики, не участвовшего в итоговой конференции по практике.

7.5. Показатели и критерии оценивания сформированности компетенций (на различных этапах их формирования), шкалы и процедуры оценивания.

Перечень компетенции	*Общее кол-во практических заданий для формируемых компетенций*	*Min кол-во заданий для выполнения*
ОК-5	*3*	*2*
ОК-6	*7*	*4*
ОК-7	*4*	*3*
ОК-8	*6*	*4*
ОК-9	*2*	*2*
ОК-11	*14*	*8*
ОК-12	*2*	*2*
ПК-1	*9*	*5*
ПК-2	*11*	*6*
ПК-3	*9*	*6*
ПК-4	*13*	*7*
ПК-5	*20*	*11*
ПК-8	*17*	*9*
ПК-9	*15*	*8*
ПК-10	*11*	*6*
ПК-11	*5*	*3*
ПК-12	*6*	*4*
ПК-13	*10*	*6*
ПК-14	*5*	*3*
ПК-15	*12*	*7*
ПК-16	*8*	*5*
ПК-19	*9*	*5*
ПК-20	*11*	*6*
ПК-24	*10*	*6*
ПК-28	*5*	*3*
ПК-29	*8*	*5*

ПК-32	*1*	*1*

8. Перечень учебной литературы и ресурсов сети "Интернет", необходимых для проведения преддипломной практики по получению профессиональных умений и опыта профессиональной деятельности

а) основная литература: (не старше 5 лет)

1. Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М. : Флинта, 2011. - 184 с.
2. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с.
3. Носов Л.С., Биричевский А.Р. Техническая защита информации. Часть 1. Инженерно-техническая защита информации. Сыктывкар: издательство Сыктывкарского государственного университета, 2012. (электронный вариант)
4. Носов Л.С., Биричевский А.Р., Едомский Д.Н. Техническая защита информации. Часть 2. Технические средства защиты информации [Электронный ресурс] / Сыктывкар: ИПО СыктГУ, 2012.
5. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. - М.: ООО "Издательство Машиностроение", 2009. - 508 с.

б) дополнительная литература: (не старше 10 лет)

1. Артемов А.В. Информационная безопасность: курс лекций / А.В. Артемов; Межрегиональная академия безопасности и выживания. - Орел: МАБИВ, 2014. - 257 с.
2. Методологические основы построения защищенных автоматизированных систем : учебное пособие / А.В. Душкин, О.В. Ланкин, С.В. Потехецкий и др. ; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». - Воронеж : Воронежская государственная лесотехническая академия, 2013. - 258 с.
3. Некраха, А.В. Организация конфиденциального делопроизводства и защита информации : учебное пособие / А.В. Некраха, Г.А. Шевцова ; Институт информационных наук и технологий безопасности, Российский государственный гуманитарный университет. - М. : Академический проект, 2012. - 222 с.
4. Сычев Ю.Н. Основы информационной безопасности: учебно-практическое пособие / Ю.Н. Сычев. - М.: Евразийский открытый институт, 2010. - 328 с.
5. Ярочкин В.И. Информационная безопасность: учебник для вузов / В.И. Ярочкин. - 5-е изд. - М.: Академический проект, 2008. - 544 с.

Учебно-методические материалы

1. Учебно-методические материалы по программе «Аттестация объектов информатизации по требованиям безопасности информации» / ГНИИ ПТЗИ ФСТЭК России. Центр повышения квалификации специалистов по ТЗИ. (Диск CD-R)
2. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. / Утвержден Первым заместителем Председателя Гостехкомиссии России 08.11.2001.

Нормативно-правовые акты

1. Конституция РФ от 12.12.1993.
2. Трудовой кодекс РФ № 197 – ФЗ от 01.02.2002.
3. Гражданский кодекс Российской Федерации часть первая от 30 ноября 1994 г. N 51-ФЗ, часть вторая от 26 января 1996 г. N 14-ФЗ, часть третья от 26 ноября 2001 г. N 146-ФЗ и часть четвертая от 18 декабря 2006 г. N 230-ФЗ.

4. Уголовный кодекс российской федерации от 13.06.1996 № 63-ФЗ.
5. Федеральный закон от 28.12.2010 N 390-ФЗ «О безопасности».
6. Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации» принятый 27 июля 2006 года.
7. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне».
8. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».
9. Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи».
10. Федеральный закон от 04.05.2011 N 99-ФЗ «О лицензировании отдельных видов деятельности».
11. Указ Президента РФ от 30.11.1995 N 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне "Перечень сведений, отнесенных к государственной тайне».
12. Постановление Правительства РФ от 06.02.2010 N 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к гостайне».
13. Указ Президента Российской Федерации от 12 мая 2009 года № 537 “О стратегии национальной безопасности Российской Федерации до 2020 года”.
14. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 года № Пр-1895.
15. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
16. Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера».
17. Указ Президента Российской Федерации от 16.08.2004 г. № 1085 Вопросы Федеральной службы по техническому и экспортному контролю.
18. Указ Президента РФ от 11.08.2003 N 960 "Вопросы Федеральной службы безопасности Российской Федерации".
19. Постановление Правительства Российской Федерации от 03 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».
20. Постановление Правительства Российской Федерации от 03 марта 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».
21. Постановление Правительства Российской Федерации от 26 июня 1995 года № 608 «О сертификации средств защиты информации».
22. Постановление Правительства Российской Федерации от 3 ноября 1994 года № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии».
23. Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требовании к защите персональных данных при их обработке в информационных системах персональных данных».
24. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
25. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
26. Постановление Правительства РФ от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

в) Интернет-ресурсы

1. http://www.fstec.ru

2. http://www.ispdn.ru
3. http://www.rsoc.ru
4. http://www.itsec.ru
5. http://www.intuit.ru
6. http:/www.biblioclub.ru
7. http://www.CyberSecurity.ru

9. Перечень информационных технологий, используемых при проведении преддипломной практики по получению профессиональных умений и опыта профессиональной деятельности, включая перечень программного обеспечения и информационных справочных систем

Для проведения преддипломной практики, для выполнения целей и задач практики необходимо:

1. Автоматизированное рабочее место
2. Справочно-правовая система КонсультатнтПлюс или Гарант
3. Программное обеспечение и технические средства защиты информации в рамках выполнения практических заданий, имеющееся на предприятии.

10. Описание материально-технической базы, необходимой для проведения преддипломной практики по получению профессиональных умений и опыта профессиональной деятельности.

Материально-техническое обеспечение преддипломной практики включает в себя:

1. Рабочее место
2. Технические и криптографические средства защиты информации в рамках выполнения практических заданий, имеющиеся на предприятии.

11. Иные сведения и материалы.

В целом в период прохождения преддипломной практики студент должен в обязательном порядке ознакомиться *со следующими вопросами*:

1. Правила техники безопасности и порядок организации труда на рабочих местах.
2. Порядок организации прохождения практики. Цель и задачи практики.
3. Требования к оформлению отчетности и защиты отчетов по практике.
4. Основные обязанности должностных лиц в области защиты информации.
5. Требования к оформлению организационно-распорядительных документов.
6. Правовые, организационные, инженерно-технические и криптографические методы защиты информации.
7. Особенности эксплуатации и состав технических, программных, аппаратных средств защиты информации.

Студент при прохождении преддипломной практики **обязан:**

- соблюдать правила охраны труда и техники безопасности;
- полностью выполнять задания, предусмотренные программой практики;
- эффективно использовать отведенное для практики время;
- качественно выполнять все практические задания;

- осуществлять сбор и анализ материалов, необходимых для подготовки отчета по практике;
- применять на практике полученные знания по изученным дисциплинам;
- представить руководителю практики письменный отчет о выполнении всех заданий и защитить его (в форме дифференцированного зачета).

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «СЫКТЫВКАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ ПИТИРИМА СОРОКИНА»
ИНСТИТУТ ТОЧНЫХ НАУК И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Кафедра информационной безопасности

Отчет
о прохождении преддипломной практики
по получению профессиональных умений и опыта профессиональной деятельности

Направление подготовки

090900 Информационная безопасность
(бакалавриат)

(Ф.И.О.)_____

Место практики_____
_____

(полное юридическое название организации, адрес)

Сроки практики_____

Выполнил:
Студент группы 133 _____ И.О. Фамилия
«____»__ __ _____20__ г.

Руководитель практики от организации _____ И.О. Фамилия
«____»__ __ _____20__ г.

Руководитель практики от кафедры _____ И.О. Фамилия
«____»__ __ _____20__ г.

Итоговая оценка по практике _____

Сыктывкар 20__г.

Приложение 2

Лист экспертной оценки

На прохождение_____практики
(название практики)

Студента (ки) ФГБОУ ВО «Сыктывкарский государственный университет им. Питирима Сорокина»

(Ф.И.О.)_____

Институт **точных наук и информационных технологий**

направление подготовки **Информационная безопасность**

Курс_____

База прохождения практики_____

_____
(полное юридическое название организации, адрес)

Должность_____
(на которую назначен или ориентирован практикант)

Сроки прохождения практики_____

Характеристика видов практической деятельности, указанных в программе практики (что сделано):

1. …
2. …
3. …

Оценка профессиональных и личностных качеств, проявленных студентом при прохождении практики

Общекультурные качества, проявленные при прохождении практики	Оценка[1] (в какой мере сформированы и проявлены)
Владение культурой мышления, способностью к аналитической деятельности	1 2 3 4 5
Владение культурой устной и письменной речи	1 2 3 4 5
Знание основных принципов деловых отношений и профессиональной этики, умение работать в коллективе	1 2 3 4 5
Умение находить организационно-управленческие решения в нестандартных ситуациях и нести ответственность за свой выбор	1 2 3 4 5

[1] 1 – не имеет никакого представления.
2 – не знает большей части теоретического материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.
3 – имеет общие представления из теории, не знает основных деталей, допускает неточности в формулировках, нарушения в последовательности изложения материала, испытывает затруднения в выполнении практических работ.
4 – твердо знает теоретический материал, не допускает существенных неточностей, обладает грамотной и логичной речью, правильно применяет творческие положения при решении практических вопросов, задач, владеет необходимыми навыками и приемами их выполнения.
5 – глубоко и прочно знает теоретический материал, исчерпывающе, грамотно, логически стройно его излагает, не испытывает трудности при выполнении практики. При этом студент не затрудняется при видоизменении задании, свободно справляется с задачами, вопросами, показывает знакомство с литературой, правильно обосновывает принятые решения. Владеет разносторонними навыками и приемами выполнения практических работ.

Умение критически оценивать свои достоинства и недостатки	1 2 3 4 5
Умение самостоятельно приобретать новые знания, стремиться к саморазвитию, повышению своей квалификации и мастерства	1 2 3 4 5
Обладание высокой мотивацией к выполнению профессиональных задач, инициативность и мобильность	1 2 3 4 5
Умение использовать информационные технологии в профессиональной деятельности. Владение знаниями в получении, хранении и переработке информации	1 2 3 4 5
Владение иностранным языком	1 2 3 4 5
Умение использовать нормативно-правовые документы в своей деятельности	1 2 3 4 5

Профессиональные умения и навыки, проявленные и приобретенные при прохождении практики	Оценка знаний, приобретенных студентом в вузе	Оценка умений и навыков, приобретенных за время прохождения практики
способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности	1 2 3 4 5	1 2 3 4 5
способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации	1 2 3 4 5	1 2 3 4 5
способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	1 2 3 4 5	1 2 3 4 5
способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	1 2 3 4 5	1 2 3 4 5
способностью применять программные средства системного, прикладного и специального назначения	1 2 3 4 5	1 2 3 4 5

Общие замечания по практике_____

_____

_____

_____

Должность руководителя практики _____ / _____/

(подпись) (расшифровка)

«___»_____201…г. ПЕЧАТЬ

Приложение 3

Текст отчета

Объем отчёта о преддипломной практике должен составлять от 6 до 20 страниц печатного текста.

Отчёт может содержать следующие разделы:

ВВЕДЕНИЕ

Место прохождения практики

Цель практики

Задачи практики

ОСНОВНАЯ ЧАСТЬ

1. Общая характеристика деятельности предприятия
2. Структура предприятия
3. Описание деятельности структурного подразделения на базе, которого осуществлялось прохождение практики
4. Формулировка задач, поставленных руководителем практики от предприятия
5. Порядок выполнения работ

ЗАКЛЮЧЕНИЕ

Выявленные особенности в работе предприятия

Рекомендации по совершенствованию системы защиты информации

Отчёт может содержать приложения:

- материалы, собранные студентом в период прохождения преддипломной практики (копии нормативно правовых и организационных документов, а также те документы, в составлении которых студент, принимал непосредственное участие в объёме, предусмотренном заданием);
- схемы, таблицы, аналитические расчёты, статистические данные и т.п.