Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное
учреждение высшего образования
«Алтайский государственный технический университет
им. И.И. Ползунова»

УТВЕРЖДАЮ
Начальник УМУ АлтГТУ
_____ Н. П. Щербаков
"29" июня 2018 г.

ПРОГРАММА ПРАКТИКИ

Вид	Производственная практика
Тип	Преддипломная практика
Содержательная характеристика (наименование)	

Код и наименование направления подготовки (специальность): 10.03.01 Информационная безопасность

Направленность (профиль, специализация): Организация и технология защиты информации

Форма обучения: очная

Статус	Должность	И.О.Фамилия	Подпись
Разработал	Доцент	Ю.Н.Загинайлов	
Рассмотрена и одобрена на заседании кафедры ИВТ и ИБ 28.06.2018 дата протокол № 11	Зав.кафедрой ИВТ и ИБ	А.Г.Якунин	
Согласовал	Декан ФИТ	А.С. Авдеев	
	Руководитель ОПОП ВО	Ю.Н. Загинайлов	
	Начальник ОПиТ	М.Н. Нохрина	

г. Барнаул

ОГЛАВЛЕНИЕ

1 Цели преддипломной практики

Преддипломная практика проводится для выполнения выпускной квалификационной работы и является обязательной.

Целями практики являются:

– формирование и закрепление общекультурных, общепрофессиональных компетенций, профессиональных компетенций в области эксплуатационной, проектно-технологической, экспериментально-исследовательской, организационно-управленческой деятельности, а также профессионально-специализированных компетенций предусмотренных ОПОП;

– осуществление или завершение исследования, разработки, проектного решения, совершенствования, связанных с тематикой ВКР, а именно технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах и процессами управления информационной безопасностью защищаемых объектов;

– контроль соответствия разрабатываемых организационных и технических компонентов, проектов организационно-распорядительной и технической документации стандартам, техническим условиям и другим нормативным документам; экспериментальное исследование подсистем и систем защиты информационных систем, проектных решений и оценка качества разработки;

– подготовка разработок к опытной эксплуатации и внедрению.

2 Задачи преддипломной практики

Задачами практики являются:

- развитие способности работать в коллективе, к самореализации и самообразованию, к коммуникации в сфере профессиональной деятельности;
- закрепление навыков использования информационных технологий, положений физики и математики, электроники, нормативных правовых актов, а также навыков определения информационных ресурсов, подлежащих защите и угроз безопасности информации на объектах защиты;
- закрепление навыков по выполнению эксплуатационной деятельности (включающих применение программных средств для решения профессиональных задач, участие в работах по реализации политик безопасности, применение комплексного подхода к обеспечению ИБ объекта защиты, участие в организации и проведении контрольных проверок работоспособности программных, программно-технических и технических средств защиты информации);
- закрепление навыков по выполнению проектно- технологической деятельности (включающих проведение анализа исходных данных для проектирования подсистем и средств защиты информации, участие в проведении тех-

нико-экономического обоснования соответствующих проектных решений, оформление рабочей технической документации);

- закрепление навыков экспериментально - исследовательской деятельности, (включающих изучение и обобщение научно-технической литературы, нормативных и методических материалов, составление обзора по вопросам обеспечения ИБ по профилю, проведение анализа ИБ объектов и систем на соответствие требованиям стандартов в области ИБ, проведение экспериментов, участие в проведении экспериментальных исследований системы защиты информации);
- закрепление знаний, умений и навыков организационно – управленческой деятельности (включающих организацию работы малых коллективов исполнителей, организацию технологического процесса защиты информации ограниченного доступа, организацию и поддержку выполнения комплекса мер по обеспечению ИБ (управление процессом их реализации));
- закрепление навыков деятельности, связанной с профилем ОПОП Организация и технология защиты информации (включающих проведение совместного анализа функционального процесса объекта защиты и его информационных составляющих, с целью определения возможных источников информационных угроз, формирование предложений по их оптимизации, тактике защиты объекта, локализации защищаемых элементов, разработку комплекса мер по обеспечению ИБ объекта, организацию контроля его защищённости).

3 Место практики в структуре основной образовательной программы

Преддипломная практика является обязательной составной частью основной профессиональной образовательной программы высшего образования в части производственных практик. Для преддипломной практики необходимы знания, умения и навыки, полученные при изучении дисциплин всех блоков учебного плана направления 10.03.01 «Информационная безопасность», а также результаты обучения, сформированные при прохождении учебных и производственных практик. Преддипломная практика подготавливает к защите выпускной квалификационной работы. Результаты преддипломной практики включаются полностью в содержание выпускной квалификационной работы.

4 Виды, типы, способы и формы проведения практики

Вид и тип практики: производственная, преддипломная (далее практика).

Форма проведения практики: дискретно по видам практик.

Способы проведения практики: стационарная и выездная. Способ проведения преддипломной практики зависит от тематики ВКР. Если тематика не связана непосредственно с деятельностью предприятия или организации, расположенных за пределами города-местоположения вуза (г.Барнаула), то способ проведения практики является стационарным. Если тематика работы связана с деятельностью организаций и предприятий, подавших заявку на прохождение практики на предприятии и расположенных в населенном пункте, отличном от местоположения вуза, то способ проведения преддипломной практики является выездным.

При использовании стационарного способа практика проводится в научных и учебных аудиториях выпускающей кафедры или подразделений АлтГТУ, на предприятиях и в организациях, с которыми заключен договор стратегического партнерства и на базе которых созданы базовые кафедры. При прохождении практики в лабораториях АлтГТУ студенты имеют свободный доступ к его образовательным ресурсам, сети Интернет, ресурсам справочно-правовых систем, также, по согласованию с материально ответственными лицами – к научному оборудованию кафедры.

При использовании выездного способа с руководством предприятия-базы практики заключается договор о направлении обучающихся на практику.

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

Практика проводится в рамках дискретной формы реализации производственных практик по направлению подготовки, после теоретического курса (8семестр) и проведения проектно -технологической практики.

С целью координации проведения практики назначается руководитель преддипломной практики от выпускающей кафедры.

5 Место, время и продолжительность проведения практики

В соответствии с учебным планом подготовки бакалавров преддипломная практика для очной формы обучения проводится на четвертом курсе (8-й семестр), сразу же после окончания второй производственной практики.

Продолжительность практики – 2 недели.

Задание и календарный план поведения практики оформляются в соответствии с приложением Б. Календарный план практики должен отражать решение ее задач применительно к тематике работы.

6 Планируемые результаты обучения при прохождении практики

В результате прохождения преддипломной практики обучающийся должен овладеть профессиональными умениями, получить опыт профессиональной деятельности, соответствующий общекультурным, общепрофессиональным, профессиональным и профессионально-специализированным компетенциям, приведенным с их декомпозицией в таблице 6.1

Таблица 6.1

Номер компетенции по ФГОС ВО	Содержание компетенции	В результате преддипломной практики обучающиеся должны:		
		знать	уметь	владеть
1	2	3	4	5
ОК-6	способность работать в коллективе, толерантно воспринимая социальные, этнические, кон-	- механизмы общения; - качества, необходимы для эффективного, бесконфликтного общения	- выбирать правильную стратегию и тактику в процессе общения	- навыками работы в коллективе

	фессиональные и культурные различия	- нравственно-этические ценности в процессе общения		
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	- грамматику русского и иностранного языков, правила речевого этикета; - иностранный язык в объеме, необходимом для осуществления перевода технических текстов и документации; - основные формы делового общения	- переводить профессиональные тексты на иностранном языке; -аргументированно устно и письменно излагать собственную точку зрения	- русским и иностранным языком на уровне, позволяющем осуществлять основные виды профессиональной деятельности; - культурой речи и навыками грамотного письма
ОК-8	способность к самоорганизации и самообразованию	-методы повышения квалификации и мастерства	- применять методы и средства познания для интеллектуального развития, повышения культурного уровня, профессионального роста; - самостоятельно осуществлять учебную деятельность в рамках будущей профессии	- навыками переоценки накопленного опыта, анализу своих возможностей, готовностью приобретать новые знания; - навыками саморазвития - навыками самостоятельной работы, способностью принимать решения в рамках своей профессиональной компетенции
ОПК-1	способность анализировать физические явления и процессы для решения профессиональных задач	основные понятия, законы и модели разделов физики, особенности физических эффектов и явлений, используемых для обеспечения защиты информации	применять основные законы физики при решении практических задач	навыками анализа физических явлений и процессов для решения задач в области защиты информации
ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач	понятия, методы, модели разделов математики, теории информации, математические методы обработки экспериментальных данных	- использовать математические методы и модели для решения прикладных задач; - строить математические модели задач профессиональной области;	основами построения математических моделей текстовой информации и моделей систем передачи информации
ОПК-3	способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач	положения электротехники, электроники и схемотехники для решения профессиональных задач	применять на практике методы анализа электрических цепей	навыками чтения электронных схем
ОПК-4	способность понимать значение информации в развитии современного общества, применять современные технологии для поиска и обработки информации способностью понимать значение информации в развитии современного общества, применять современные технологии для поиска и обработки	основные понятия информатики, информационные технологии для поиска и обработки информации, назначение, функции и структуру аппаратных СВТ, ОС, СУБД, вычислительных сетей	использовать программные и аппаратные средства персонального компьютера	навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.);

	информации			
ОПК-5	способность использовать нормативные правовые акты в профессиональной деятельности	основы организационного и правового обеспечения ИБ, основные НПА в области обеспечения ИБ и нормативные методические документы ФСБ России и ФСТЭК России в области ИБ и защиты информации	применять нормативные правовые акты и нормативные методические документы в области обеспечения ИБ	навыками работы с нормативными правовыми актами, в том числе по технической защите информации
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	- современные виды информационного взаимодействия и обслуживания; - основные угрозы безопасности информации и модели нарушителя в ИС	- разрабатывать модели угроз и нарушителей информационной безопасности ИС - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - выявлять уязвимости информационно-технологических ресурсов ИС	- навыками анализа информационной инфраструктуры ИС и ее безопасности - методами выявления угроз информационной безопасности ИС
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	современные виды информационного взаимодействия и обслуживания. - аппаратные средства вычислительной техники. - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные сети и системы передачи информации. - основные задачи и понятия криптографии; - требования к шифрам и основные характеристики шифров; - модели шифров и математические методы их исследования; - принципы построения криптографических алгоритмов	- осуществлять удаленный доступ к базам данных. - использовать программные и аппаратные средства персонального компьютера. - проводить анализ показателей качества сетей и систем связи. - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. - использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки; - уметь пользоваться научно-технической литературой в области криптографии.	-навыками безопасного использования технических средств в профессиональной деятельности. - методикой анализа сетевого трафика. - криптографической терминологией; - навыками использования ПЭВМ в анализе простейших шифров; - навыками математического моделирования в криптографии.
ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	- современные средства разработки и анализа ПО на языках высокого уровня; - методы программирования и методы разработки эффективных алгоритмов решения прикладных задач; - основы администриро-	- формализовать поставленную задачу, выбирать необходимые инструментальные средства для разработки программ в различных ОС и средах; - составлять, тестировать, отлаживать	- навыками разработки программ на языке программирования высокого уровня

		вания ОС и вычислительных сетей; - эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы	и оформлять програм-мы на языках высокого уровня; - устанавливать и осуществлять первичную настройку одной из ОС	
ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты	- принципы организации информационных систем в соответствии с требованиями по защите информации - криптографические стандарты и их использование в информационных системах..	- развертывать, конфигурировать и настраивать вычислительные сети. - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе. - применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	- навыками использования типовых криптографических алгоритмов.
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	принципы формирования политики информационной безопасности в информационных системах	- разрабатывать частные политики информационной безопасности информационных систем; - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения ИБ ИС	- навыками разработки политик безопасности информационных систем применительно к технологиям защиты - навыками организации разработки и формирования разделов концепции защиты информации на объекте информатизации
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	- организацию работы и нормативные правовые акты и стандарты по аттестации объектов информатизации.	- выбирать необходимые методики и документы по аттестации объектов информатизации	- методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности.
ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных,	методы и средства контроля эффективности технической защиты информации	контролировать эффективность принятых мер по реализации частных политик информационной безопасности ин	- навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем (аудита)

	программно-аппаратных и технических средств защиты информации		формационных систем.	
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	- основные методы, модели и стандарты управления информационной безопасностью; - этапы и порядок проектирования защищённых ИС; - структуру и содержание технического задания и технического проекта на защищённую ИС; -методику технико-экономического обоснования проектных решений	- оценивать информационные риски в информационных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем.	- методами управления информационной безопасностью информационных систем; - методами оценки информационных рисков; - навыками участия в технико-экономическом обосновании проектных решений
ПК-8	способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	-свойства, функции и признаки документа, в том числе как объекта нападения и защиты; - основы документационного обеспечения управления задачи органов защиты информации на предприятиях; - организацию работы и нормативные правовые акты по сертификации средств защиты информации.	- квалифицированно исследовать состав документации предприятии (организации); разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации.	методами формирования требований по защите информации
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	- основы систематизации научно-технической литературы, её основные электронные базы в области ИБ и защиты информации; -нормативные и методические материалы (документы) и электронные базы их хранения; - основы реферирования научной и специальной литературы, анализа нормативных и методических источников	-составлять аналитические обзоры по вопросам обеспечения безопасности информационных систем ИС и организации защиты информации на объектах информатизации	навыками изучения и обобщения научно-технической литературы, составления обзоров по вопросам обеспечения безопасности ИС и организации защиты информации на объектах информатизации
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	знать отечественные изарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.	навыками применения стандартов в области компьютерной безопасности для оценки защищённости компьютерных систем
ПК-11	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	методику проведения физического эксперимента и обработки его результатов. методы расчета и инструментального контроля показателей технической защиты	- проводить физический эксперимент и обрабатывать его результаты - проводить расчет и инструментальный контроль показателей техни-	- навыками проведения физического эксперимента и обработки его результатов - методами расчета и инструментального контроля показателей технической защиты

		информации	ческой защиты информации.	информации.
ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации	технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации	- анализировать и оценивать угрозы информационной безопасности объекта - проводить мониторинг угроз безопасности информационных систем.	- методами и средствами выявления угроз безопасности ИС; - методами технической защиты информации; - методами формирования требований по защите информации; - методами мониторинга и аудита угроз ИБ ИС
ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	- принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации)	-планировать, поддерживать и контролировать выполнение мер по обеспечению ИБ персоналом	- методами организации и управления деятельностью служб защиты информации на предприятии.
ПК-14	способность организовать работу малого коллектива исполнителей в профессиональной деятельности	- основные понятия и методы в области управленческой деятельности; - содержание управленческой работы руководителя подразделения.	- осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач.	- навыками обоснования, выбора, реализации и контроля результатов управленческого решения.
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 экспертному контролю	-правовые основы организации защиты информации ограниченного доступа, задачи органов защиты информации на предприятиях; -организацию работы и НПА по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации. - нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации.	организовать разработку и внедрение документов регламентирующих организационные мероприятия и технические меры защиты информации ограниченного доступа	навыками организации и документационного обеспечения режима конфиденциальности информации
ПСК2-1	способность проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников информационных угроз, их вероятных целей и тактики	- знать структуры функциональных процессов ИС (государственных, персональных данных) и защищаемых помещений, их информационных составляющих и методики определения информационных угроз для них	- проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников информационных угроз, их вероятных целей и тактики	- навыками определения возможных источников информационных угроз, их вероятных целей и тактики для ИС (государственных, персональных данных) и защищаемых помещений

ПСК2-2	способность формировать предложения по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов	- технологии безопасной архитектуры ОС, СУБД, вычислительных сетей; - способы оптимизации функционального процесса и его информационных составляющих для повышения их устойчивости к деструктивным воздействиям на информационные ресурсы ; - технологии защиты объекта (ИС – государственных, персональных данных, защищаемых помещений)	- формировать предложения по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на ин–формационные ресурсы; - формировать предложения по тактике защиты объекта и локализации защищаемых элементов	-навыками формирования предложений по тактике защиты объекта и локализации защищаемых элементов
ПСК2-3	способность разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение	- технологии комплексного обеспечения защиты информации на объекте информатизации	применять технологии комплексного обеспечения защиты информации на объекте информатизации	навыки формирования комплекса мер по обеспечению информационной безопасности объекта
ПСК2-4	способностью организовать контроль защищенности объекта в соответствии с нормативными документами	- методы, методики контроля защищённости; - нормативные документы по защите информации	организовать контроль защищенности объекта в соответствии с нормативными документами	навыками контроля защищенности объекта в соответствии с нормативными документами

7 Структура и содержание практики

Общая трудоемкость преддипломной практики составляет 3 зачетных единицы, или 108 часов.

Преддипломная практика является заключительным практическим этапом получения профессиональных навыков и умений в эксплуатационной, проектно-технологической, экспериментально - исследовательской, организационно-управленческой, профессионально-специализированной деятельности. Во время преддипломной практики осуществляется или завершается выполнение индивидуального задания по теме выпускной квалификационной работы.

В области эксплуатационной деятельности обучающийся в период прохождения преддипломной практики должен выполнить:

- завершение проектирования программных средств в соответствии с заданием;
- разработку и оформление политики безопасности информационной системы и (или) сформировать разделы концепции защиты информации на объекте информатизации;
- осуществить контрольные проверки работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации и (или) аудит безопасности информационной системы.

В области проектно-технологической деятельности обучающийся в период прохождения преддипломной практики должен:

- завершить анализ исходных данных для проектирования подсистем и средств обеспечения ИБ и технико-экономическое обоснование соответствующего проектного решения (решений);

- реализовать применение современных инструментальных средств разработки программно-аппаратного обеспечения, включая web-технологии;
- оформить проекты организационно- распорядительных и методических документов и (или) рабочую техническую документацию с учетом действующих нормативных и методических документов;

В области экспериментально - исследовательской деятельности обучающийся в период прохождения преддипломной практики должен:

-завершить подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, обзор по вопросам в соответствии с темой ВКР;

- выполнить анализ информационной безопасности объекта и (или) системы на соответствие требованиям стандартов в области информационной безопасности;
- выполнить экспериментальные исследования системы защиты информации (в части технической защиты информации от утечки по техническим каналам и (или) по инфо-телекоммуникационным каналам);
- подготовить разработку к внедрению, разработанный программный продукт – к регистрации в Роспатенте.

В области организационно-управленческой деятельности обучающийся в период прохождения преддипломной практики должен:

- выполнить разработку документационного обеспечения режима конфиденциальности информации.

Конкретные работы в период преддипломной практики согласуются с темой ВКР и текущим этапом жизненного цикла объектов профессиональной деятельности.

График учебного процесса по практике приведен в таблице 7.1.

Таблица 7.1.

Разделы (этапы) практики	Виды учебной работы на практике и их трудоемкость в часах	Формы текущего контроля
Подготовительный	Инструктаж по технике безопасности 2	Фиксация в журнале
Экспериментальный	Проектирование, разработка, модернизация, исследование объектов профессиональной деятельности, соответствующих теме ВКР 60	Представление руководителю результатов (раз в 3 дня)
Обработка и анализ полученной информации	Оценка качества разрабатываемых или модернизируемых объектов профессио-	Представление руководителю результатов (по завершении практики)

	нальной деятельности 10	
Обработка и анализ полученной информации	Контроль соответствия проектов и документации нормативным документам 20	Нормоконтроль
Подготовка и сдача отчета по практике	Оформление материалов 16	Защита
ИТОГО	108	

8 Перечень информационных технологий, используемых при проведении преддипломной практики

При прохождении преддипломной практики используются следующие технологии:

– Интернет - технологии;

– сетевые технологии;

– технологии осуществления эксплуатационной, проектно-технологической, экспериментально-исследовательской и организационно-управленческой деятельности;

– технология мастер-классов;

– технология проблемного обучения путем инициирования самостоятельного поиска студентом знаний через проблематизацию преподавателем учебного материала;

– технология контекстного обучения путем интеграции различных видов деятельности студентов: учебной, научной, практической и создания условий, максимально приближенных к реальным.

9 Учебно-методическое обеспечение самостоятельной работы студентов на практике

Учебно-методическое обеспечение самостоятельной работы студентов на преддипломной практике осуществляется свободным доступом студентов к библиотечным фондам ВУЗа и базам данных кафедры, а также свободным доступом к необходимой компьютерной технике и оборудованию, имеющимся в распоряжении кафедры и в лабораториях.

Организацию и проведение практики обеспечивают университет и выпускающая кафедра. В случае прохождения практики в сторонней организации, ее руководство в соответствии с договором обеспечивает доступ обучаемого к технике, документации, программному и аппаратному обеспечению, требующимся для выполнения задания по практике.

Кафедра определяет сроки защиты практики с учетом утвержденного графика учебного процесса. На основании изданного приказа студентам, убывающим на практику, выдается программа практики и методические рекомендации по ее выполнению.

Общее организационное и учебно-методическое руководство практикой студентов осуществляет преподаватель-руководитель практики от вуза.

Преподаватель-руководитель практики:

– проводит собрание студентов учебно-производственной группы, где подробно объясняет цели, задачи, значение и порядок прохождения практики;

– проводит консультации и оказывает помощь студентам по вопросам практики;

– контролирует процесс прохождения практики обучающимися, принимает меры к устранению причин и условий, способствовавших недобросовестному отношению студентов к своим обязанностям;

– контролирует соблюдение сроков прохождения практики и ее содержание;

– предварительно оценивает результаты выполнения обучающимися программы практики с учетом отзыва научного руководителя по теме ВКР и/или специалиста предприятия-базы практики.

Перед началом производственной практики студент получает программу практики, индивидуальное задание на практику (см. приложение Б), необходимую документацию для выполнения задания.

Обучающийся должен демонстрировать руководителю практики результаты работы не реже, чем раз в три календарных дня. Задания по практике выполняются студентом самостоятельно и индивидуально. По согласованию с руководством кафедры разработка ВКР может выполняться двумя обучающимися, но в этом случае каждый студент выполняет свое задание на практику. В течение практики студент консультируется у руководителя практики, у научного руководителя, у специалистов предприятия-базы практики.

10 Формы промежуточной аттестации по итогам практики

10.1 Оформление отчета по практике

Во время практики студент должен не менее одного раза в три дня предоставлять руководителю практики результаты своей работы.

По окончании практики обучающийся составляет письменный отчет и сдает его руководителю практики от университета вместе с календарным планом. Календарный план подписывается руководителем от вуза и научным руководителем ВКР (руководителем практики от организации).

Студенты, не выполнившие программы практики по уважительной причине, не допускаются к выполнению выпускной квалификационной работы.

Отчет о практике должен содержать:

– титульный лист, оформленный согласно приложению А;

– задание и календарный план выполнения практики, подписанные научным руководителем и руководителем практики, оформленный согласно приложению Б;

– введение;

– первый раздел - описание предметной области, известных научно-исследовательских и технических разработок, анализ объекта защиты;

– второй раздел – исследования уязвимости объекта и его элементов, разработка модели угроз безопасности информации, расчёт рисков, определение требований НПА и стандартов к технической защите объекта, алгоритмы и структуры данных при разработке ПО;

– третий раздел – комплексные решения по защите информации объекта информатизации или организации, разработанные компоненты (подсистемы) системы защиты объекта или разработанные средства защиты, состав и структура организационно-распорядительных, методических, рабочих и технических документов, описание ПО при разработке программ;

– заключение;

– список использованных источников информации;

– приложение (необязательно).

Введение должно содержать краткое обоснование актуальности тематики, которой посвящена ВКР (объем не более 1 страницы).

Первый раздел включает 15-20 страниц. В разделе дается описание предметной области исследований, анализ объекта (функционального процесса объекта) защиты информации (включая информационные потоки), описание и критический анализ аналогичных разработок по защите объекта и исследований по теме ВКР, обоснование актуальности разработки.

Второй раздел включает 15-20 страниц. Если разрабатываются (совершенствуются) элементы (подсистемы) технической защиты информации от утечки по техническим каналам, то во втором разделе рассматривается модель угроз. Определяются требования к разрабатываемым подсистемам или средствам в соответствии с НПА и стандартами, методическими документами ФСБ и ФСТЭК России.

Если разрабатываются (совершенствуются) элементы (подсистемы) технической защиты информации в информационных системах и в информационно-телекоммуникационных сетях должны быть представлены модели угроз и нарушителей и элементы экспериментальных исследований системы защиты.

Третий раздел включает 15-20 страниц. В этом раздел приводятся результаты проектирования средств или компонентов (подсистем) системы защиты объекта или проектные решения для системы защиты. Здесь рассматриваются методики, технологии разработки структура и содержание политик информационной безопасности, концепций комплексной защиты объекта информатизации, комплексные решения по защите информации объекта информатизации или организации, разработанные компоненты (подсистемы) системы защиты объекта или разработанные средства защиты, состав и структура организационно-распорядительных, методических, рабочих и технических документов, технико-экономическое обоснование проектных решений, описание ПО при разработке программ, результаты исследования защищённости объектов информатизации и эффективности их систем защиты.

В разделе “Заключение” (0,5-1 страница) студент должен кратко изложить результаты выполненной работы.

В приложение к отчету выносится текст программы и (или) проекты разработанных документов различного назначения (политики безопасности, концепции, положения, инструкции, технические паспорта, другие).

Общий объем отчета должен составлять 35-45 страниц печатного текста. Текст отчета оформляется в виде принтерных распечаток на сброшюрованных листах формата А4 (210х297мм). При оформлении отчета необходимо соблюдать требования ГОСТ 2.105, ГОСТ 2.106, ГОСТ 3.1127, ГОСТ 3.1123, ГОСТ 3.1407, ГОСТ 8.417, ГОСТ 7.1, СТО 12 570-2013 Общие требования к текстовым, графическим и программным документам.

Оценка по практике выставляется на основе результатов сдачи студентами отчётов о практике в соответствии с СК ОПД 01-19-2018 Положение о модульно-рейтинговой системе квалиметрии учебной деятельности студентов.

К защите отчётов допускаются студенты, полностью выполнившие программу практики и представившие отчёт о практике в соответствии с требованиями СТО АлтГТУ 12 330-2016 Практика. Общие требования к организации, проведению и программе практики.

Сдача отчёта о практике осуществляется на последней неделе практики, в последний и предпоследний день. Допускается сдача отчёта о практике в более поздние сроки, но не позднее дня, предшествующего государственной итоговой аттестации.

Студентам, успешно сдавшим отчёт о практике, в ведомости и в зачётные книжки выставляется зачёт с оценкой («отлично», «хорошо», «удовлетворительно»), а также рейтинг в диапазоне 25-100 баллов (определяется в соответствии с Положением о модульно-рейтинговой системе квалиметрии учебной деятельности студентов в АлтГТУ) с учётом мнения руководителя практики, полноты и качества отчета, результатов сдачи отчета, других материалов (например, характеристики с места практики).

10.2 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

В таблицу 10.1 сведен перечень компетенций, частичное формирование которых происходило до начала прохождения преддипломной практики.

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

Код контролируемой компетенции	Этап формирования компетенции	Способ оценивания	Оценочное средство
ОК-6. Способность работать в коллективе, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
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 профессиональ-	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике

ной деятельности			
ОК-8 способность к самореализации и самообразованию	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ОПК-1: способность анализировать физические явления и процессы для решения профессиональных задач	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ОПК-3: способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ОПК4: способность понимать значение информации в развитии современного общества, применять современные технологии для поиска и обработки информации	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-3: способность администриро-	итоговый	зачет с оцен-	Комплект контро-

вать подсистемы информационной безопасности объекта защиты		кой	лирующих материалов и иных заданий для защиты отчёта о практике
ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-5: способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-6: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
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	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
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	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-11 способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о

			практике
ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-13: способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-14: способность организовать работу малого коллектива исполнителей в профессиональной деятельности	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
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 экспертному контролю	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПСК2-1: способность проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью *определения* возможных источников информационных угроз, их вероятных целей и тактики	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПСК2-2: способность формировать предложения по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПСК2-3: способность разработать комплекс мер по обеспечению информационной безопасности *объекта и организовать его внедрение* и последующее сопровождение	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПСК2-4: способность организовать контроль защищенности объекта в соответствии с нормативными документами	итоговый	зачет с оценкой	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике

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

Критерий	Оценка по 100-балльной шкале	Оценка
При защите отчета студент показал глубокие знания вопросов темы, свободно оперировал данными исследования и внес обоснованные предложения. Студент правильно и грамотно ответил на все поставленные вопросы. Практикант получил положительный отзыв от руководителя практики. Отчет в полном объеме соответствует заданию на практику.	75-100	*Отлично*
При защите отчета студент показал знания вопросов темы, оперировал данными исследования, внес обоснованные предложения. В отчете были допущены ошибки, которые носят несущественный характер. Практикант получил положительный отзыв от руководителя практики.	50-74	*Хорошо*
Отчет по практике имеет поверхностный анализ собранного материала, нечеткую последовательность изложения материала. Студент при защите отчета по практике не дал полных и аргументированных ответов на заданные вопросы. В отзыве руководителя практики имеются существенные замечания.	25-49	*Удовлетворительно*
Отчет по практике не имеет детализированного анализа собранного материала и не отвечает требованиям, изложенным в программе практики. Студент затрудняется ответить на поставленные вопросы или допускает в ответах принципиальные ошибки. В полученной характеристике от руководителя практики имеются существенные критические замечания.	<25	*Неудовлетворительно*

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

Для оценки знаний, умений и навыков, характеризующих этапы формирования компетенций в период преддипломной практики, используются следующие **типовые контрольные вопросы:**

1. Что послужило основой выбора объекта защиты информации в рамках индивидуального задания? (ОК-8).
2. Как Вы оцениваете свою готовность к работе в коллективе? (ОК-6).
3. Вы считаете полученные за время практики результаты значительными? Почему? (ОК-8).

4. Какие законы физики и физические процессы использовались Вами для экспериментальных исследований и разработки проектных решений? Почему? (ОПК-1).

5. Использовался ли для разработки проектных решений математический аппарат и в частности математическое моделирование? (ОПК-2).

6. Какие положения электроники и схемотехники использованы вами для разработки электронных схем? (ОПК-3).

7. Решались ли ранее задачи, поставленные Вами и являются ли они актуальными? (ОПК-4).

8. Какие способы решения поставленных задач Вам известны, какие исследователи занимались данными проблемами? (ПК-9).

9. Какие отечественные и зарубежные научно-технические журналы и Интернет источники Вами проанализированы? (ОПК-4).

10. Какие сайты профессиональной направленности Вы периодически посещаете? (ОПК-4).

11. Поясните, какой математический аппарат используется при оценке рисков информационной безопасности в организации и каков практический опыт его применения? (ОПК-2).

12. Какие специализированные сайты сети «Интернет» и информационные ресурсы в области информационной безопасности Вы использовали при решении задач определённых в работе? (ОПК-4).

13. Нормы каких нормативных правовых актов, и какие Вы использовали для решения задач поставленных в работе? (ОПК-5).

14. Приведите правовое обоснование для сформированного Вами комплекса мер по информационной безопасности. (ОПК-5).

15. Какие угрозы информационной безопасности характерны только для объектов рассматриваемого Вами объекта информатизации, обусловленные спецификой его деятельности? (ПСК2-1).

16. Какие предложения сформированы Вами по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы? (ПСК2-2).

17. Какие методы анализа уязвимостей и угроз вы использовали в интересах разработки проектных решений? (ПК-7).

18. Какие элементы включает подсистема управления информационной безопасностью объекта защиты (организации)? (ПК-15).

19. Какие факторы и особенности объекта защиты повлияли на формирование организационно-распорядительных и методических документов для подсистемы управления информационной безопасностью? (ПК-13).

20. Какие результаты дал предварительный технико-экономический анализ компонентов (системы) защиты организации и как он повлиял на обоснование проектного решения по обеспечению информационной безопасности? (ПК-7).

21. Какие нормативные и методические документы в области информационной безопасности Вы использовали при разработке технической документации? (ПК-8).

22. Чем отличаются Ваши алгоритмы для разработки программы от уже известных? (ПК-3)

23. Поясните выбор среды разработки ПО, в чем ее достоинства и недостатки? (ПК-2).

24. Какие инструментальные средства и системы программирования были проанализированы для решения Ваших задач? (ПК-3).

25. Почему вы выполнили программную реализацию криптографического алгоритма именно на этом языке программирования? (ПК-2).

26. Планируется ли регистрация авторских прав на созданные объекты интеллектуальной собственности? (ОК-8).

27. Какие исходные данные положены в основу Вашего проектного решения подсистемы (средства) обеспечения информационной безопасности. (ОПК-7).

28. Обзор каких средств защиты вы провели и как он повлиял на выбор средств используемых в Вашей работе? (ПК-9).

29. Какие отечественные и зарубежные стандарты вы использовали для анализа информационной безопасности объектов (системы)? (ПК-10).

30. На основе каких критериев или принципов вы осуществили выбор (изучение и обобщение научно-технической литературы), нормативных и методических материалов для решения вопроса обеспечения информационной безопасности? (ПК-9).

31. Какие экспериментальные исследования вы провели в интересах совершенствования и разработки технических компонентов системы защиты информации? (ПК-11).

32. Какие вы лично разработали предложения по совершенствованию системы управления информационной безопасностью? (ПК-1)

33. Покажите экономическую целесообразность применения Вами выбранного средства защиты информации. (ПК-7).

34. Как в вашей работе реализован комплексный подход к обеспечению информационной безопасности и как в нём учтена сфера деятельности предприятия? (ПСК2-1).

35. Что включает предложенный Вами комплекс мер по обеспечению информационной безопасности объекта в части организационной составляющей? (ПСК2-3).

36. На основе каких нормативных документов Вы организовывали контроль защищённости объекта информатизации? (ПСК2-4)

Комиссией могут быть заданы вопросы, касающиеся как исследуемых, модернизируемых, проектируемых, реализуемых, анализируемых объектов профессиональной деятельности, так и общие вопросы в области информационно-коммуникационных технологий и технологий информационной безопасности.

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

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и(или) опыта деятельности, характеризующих этапы формирования компетенций, определены локальными нормативными актами СТО АлтГТУ

12100-2015 Фонд оценочных средств образовательной программы. Общие требованияия, СТО АлтГТУ 12330-2016 Практика. Общие требования к организации, проведению и программе практики и СК ОПД 01-19-2018 Положение о модульно-рейтинговой системе квалиметрии учебной деятельности студентов.

Обучающимся, успешно защитившим отчет о практике, в ведомости и в зачётные книжки выставляется зачёт с оценкой «отлично», «хорошо», «удовлетворительно», а также рейтинг в диапазоне 25 - 100 баллов с учетом мнения руководителя практики, научного руководителя, полноты и качества отчёта, результатов защиты, дополнительных материалов (например, характеристики с места практики).

Обучающимся, не выполнившим программу практики, или не защитившим, по мнению комиссии, отчёт, в ведомости выставляется «неудовлетворительно». Если программа практики не выполнена без уважительных причин или студент не защитил отчёт, он считается неуспевающим.

Обучающийся, не выполнивший программу преддипломной практики по уважительной причине, направляется на практику повторно в свободное от учёбы время.

Если результаты защиты отчёта о практике признаны неудовлетворительными, комиссия принимает решение о возможности повторной защиты и её дате и сообщает о своём решении в деканат. Повторная защита практики проводится аналогично ликвидации задолженностей по зачету в трехдневный срок, в связи с необходимостью получения допуска к выполнению выпускной квалификационной работы.

Для обучающихся, не выполнивших программу практики по неуважительной причине, а также для студентов, по которым комиссия признала нецелесообразным повторную защиту отчёта о практике, ее повторное прохождение в сроки, отличные от указанных в графике, возможно только с разрешения проректора по учебной работе (по формам обучения). При наличии разрешения практика реализуется в свободное от учёбы время.

Обучающиеся, не выполнившие программу практики без уважительных причин, получившие на защите отчета о практике неудовлетворительную оценку и не получившие разрешения на повторное прохождение практики или повторную защиту отчета, представляются к отчислению как имеющие академическую задолженность.

11 Учебно-методическое и информационное обеспечение практики

1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

2. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040 .

3. Малюк, А.А. Теория защиты информации [Электронный ресурс] : . — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 184 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5170 — Загл. с экрана.

4. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. [электронный ресурс]/Изд-во "ДМК Пресс", 2012. 592 с. – доступ из ЭБС «Лань» - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=3032 - Загл. с экр.

5. Технические методы и средства защиты информации [электронный ресурс]/Под ред. А.П. Зайцева. - М.:2012 г.- доступ из ЭБС «Лань» - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5154 - Загл. с экр.

6. Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 [Электронный ресурс] : учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 244 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5178 — Загл. с экрана.

Дополнительная литература:

7. Грибунин В.Г. Комплексная система защиты информации на предприятии: учебник для студ. высш. учеб. заведений./ В.Г.Грибунин, В.В. Чудовский.- М.: Издательский центр «Академия», 2008.-320с. (25 экз. Гриф УМО); 2009 – 412

8. Обработка и обеспечение безопасности электронных данных : учебное пособие / А.В. Агапов, Т.В. Алексеева, А.В. Васильев и др. ; под общ. ред. Д.В. Денисов. - М. : Московский финансово-промышленный университет «Синергия», 2012. - 592 с. : ил., табл. - (Сдаем госэкзамен: ответы на экзаменационные вопросы). - ISBN 978-5-4257-0074-2 ; То же [Электронный ресурс]. - URL:http://biblioclub.ru/index.php?page=book&id=252894

9. Лапина, М.А. Информационное право : учебное пособие / М.А. Лапина, А.Г. Ревин, В.И. Лапин ; под ред. И.Ш. Килясханова. - М. : Юнити-Дана, 2015. - 336 с. - (Высшее профессиональное образование: Юриспруденция). - Библиогр. в кн. - ISBN 5-238-00798-1 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=118624 (13.02.2017).

Программное обеспечение и интернет ресурсы:

10. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [электронный ресурс]:- режим доступа: http:// www.fstec.ru.

11. Официальный сайт федерального агентства по техническому регулированию и метрологии [электронный ресурс]: режим доступа: http://protect.gost.ru//

12. Правовая справочная система «Гарант» [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ. (Платформа F1 Гарант); 2. http://www.garant.ru

13. Искусство управления информационной безопасностью. Профессиональный сайт [электронный ресурс]:- режим доступа http://www.iso27000.ru/

14. Портал в области компьютерной безопасности. [электронный ресурс]:- режим доступа http://www.securitylab.ru/news/485237.php

12 Материально-техническое обеспечение практики

Для проведения практики используются компьютерные классы и лаборатории кафедры ИВТ и ИБ, а также учебно-лабораторная и производственная база предприятий-баз практики.

Кафедра ИВТ и ИБ предоставляет для преддипломной практики: компьютеры с установленными средами разработки программного обеспечения и доступом в интернет, оборудование лабораторий кафедры.

ПРИЛОЖЕНИЕ А
Форма титульного листа отчета о практике

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
”Алтайский государственный технический университет им. И. И. Ползунова”

Факультет информационных технологий
наименование подразделения

Кафедра информатики, вычислительной техники и информационной безопасности
наименование кафедры

Отчет защищен с оценкой_____
“____”_____20___г.
Руководитель от университета
_____ / _____/
подпись Ф. И. О.

ОТЧЕТ

о производственной, преддипломной практике

_____
общая формулировка задания

в _____
наименование организации

Студент гр. ИБ-31_____Иванов П.С._____
индекс группы подпись Ф. И. О.

Руководитель от организации _____ _____
подпись Ф. И. О.

Руководитель от университета _____ _____
подпись Ф. И. О.

201_

ПРИЛОЖЕНИЕ Б
Форма задания и календарного плана практики

ФГБОУ ВО «Алтайский государственный технический университет им. И. И. Ползунова»
Кафедра Кафедра информатики, вычислительной техники и информационной безопасности

Индивидуальное задание

на производственную, преддипломную практику
(вид, тип и содержательная характеристика практики по УП)

студенту _4___ курса _____ группы _____
(Ф.И.О.)

Профильная организация_____
(наименование)

Сроки практики _____
(по приказу АлтГТУ)

Тема _____
_____

Рабочий график (план) проведения практики:

№ п/п	Содержание раздела (этапа) практики	Сроки выполнения	Планируемые результаты практики

Руководитель практики от университета _____ _____
(подпись) (Ф.И.О., должность)

Руководитель практики от профильной организации _____ _____
(подпись) (Ф.И.О., должность)

Задание принял к исполнению _____ _____
(подпись) (Ф.И.О.)