Федеральное государственное бюджетное образовательное учреждение высшего образования
«Алтайский государственный технический университет им. И.И. Ползунова»

Рабочая программа практики

Вид	Производственная практика
Тип	Преддипломная практика

Код и наименование направления подготовки (специальности): **10.03.01 Информационная безопасность**

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

Форма обучения: **очная**

Статус	Должность	И.О. Фамилия
Разработал	заведующий кафедрой	А.Г. Якунин
Согласовал	Зав. кафедрой «ИВТиИБ»	А.Г. Якунин
	Декан ФИТ	А.С. Авдеев
	руководитель ОПОП ВО	Е.В. Шарлаев

г. Барнаул

1. ВИД, ТИП, СПОСОБ и ФОРМА ПРОВЕДЕНИЯ ПРАКТИКИ

Вид: Производственная
Тип: Преддипломная практика
Способ: стационарная и (или) выездная
Форма проведения: путем чередования с реализацией иных компонентов образовательной программы в соответствии с календарным учебным графиком и учебным планом
Форма реализации: практическая подготовка

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
ОК-6	способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	- механизмы общения; - качества, необходимы для эффективного, бесконфликтного общения - нравственно-этические ценности в процессе общения	- выбирать правильную стратегию и тактику в процессе общения	- навыками работы в коллективе
ОК-7	способностью 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	способностью 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

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
				компетенции
ОПК-1	способностью 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	способностью 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	способностью 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	способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	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.)
ОПК-5	способностью использовать нормативные правовые акты в профессиональной деятельности	основы организационного и правового обеспечения ИБ, основные НПА в области обеспечения ИБ и нормативные методические	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

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
		документы ФСБ России и ФСТЭК России в области ИБ и защиты информации		
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	- современные виды информационного взаимодействия и обслуживания; - основные угрозы безопасности информации и модели нарушителя в ИС	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	способностью 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;	-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

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
			- уметь пользоваться научно-технической литературой в области криптографии	
ПК-2	способностью 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 администрирования ОС и вычислительных сетей; - эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы	- формализовать поставленную задачу, выбирать необходимые инструментальные средства для разработки программ в различных ОС и средах; - составлять, тестировать, отлаживать и оформлять програм-мы на языках высокого уровня; - устанавливать и осуществлять первичную настройку одной из ОС	- навыками разработки программ на языке программирования высокого уровня
ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты	- принципы организации информационных систем в соответствии с требованиями по за-щите 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	- навыками использования типовых криптографических алгоритмов

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
			компьютерных систем	
ПК-4	способностью 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	способностью 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	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	методы и средства контроля эффективности технической защиты информации	контролировать эффективность принятых мер по реализации частных политик информационной безопасности ин формационных систем	- навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем (аудита)
ПК-7	способностью 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-	- 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

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
		экономического обоснования проектных решений		
ПК-8	способностью 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; - организацию работы и нормативные правовые акты по сертификации средств защиты ин-формации	- 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	способностью 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	способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	знать отечественные и зарубежные 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	способностью проводить эксперименты по	методику проведения	- проводить	- навыками

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
	заданной методике, обработку, оценку погрешности и достоверности их результатов	физического эксперимента и обработки его результатов. методы расчета и инструментального контроля показателей технической защиты информации	физический эксперимент и обрабатывать его результаты - проводить расчет и инструментальный контроль показателей технической защиты информации	проведения физического эксперимента и обработки его результатов - методами расчета и инструментального контроля показателей технической защиты информации
ПК-12	способностью 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	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	- принципы формирования комплекса мер по обеспечению ин-формационной 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	способностью организовывать 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	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными	-правовые основы организации защиты информации ограниченного доступа, задачи органов защиты информации на предприятиях; -организацию работы	организовать разработку и внедрение документов, регламентирующих организационные мероприятия и технические меры защиты	навыками организации и документационного обеспечения режима конфиденциальности информации

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
	методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	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	информации ограниченного доступа	
ПСК2-1	Способность проводить совместный анализ функционального процесса объекта защиты н 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

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
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	- навыками формирования комплекса мер по обеспечению информационной безопасности объекта
ПСК2-4	Способность 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

3. ОБЪЕМ ПРАКТИКИ

Общий объем практики – 3 з.е. (2 недель)
Форма промежуточной аттестации – Зачет с оценкой.

4. СОДЕРЖАНИЕ ПРАКТИКИ

Семестр: 8

Форма промежуточной аттестации: Зачет с оценкой

Разделы (этапы) практики	Содержание этапа практики
1.Инструктаж по технике безопасности(2ч.)	
2.Информационно-аналитический {с элементами электронного обучения и дистанционных образовательных технологий} (16ч.)[1,2,7,8,9]	Информационный поиск по выявлению и анализу существующих аналогичных решений в близкой к теме ВКР области с применением современных технологий для поиска и обработки информации. Подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов. Анализ информационной безопасности соответствующих теме ВКР объектов и систем на соответствие требованиям стандартов в области информационной безопасности. Анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников информационных угроз, их вероятных целей и тактики. Определение информационных ресурсов, подлежащих защите, угрозы безопасности информации и пути их реализации на основе анализа структуры и содержания

	информационных процессов и особенностей функционирования объекта защиты.
3.Проектно-технологический {творческое задание} (36ч.)[3,4,5,6]	Проектирование, разработка, модернизация, исследование объектов профессиональной деятельности, соответствующих теме ВКР, в том числе подсистем и средств обеспечения информационной безопасности по результатам анализа исходных данных и результатов информационного поиска. Применение программных средств системного, прикладного и специального назначения, инструментальных и технических средств, языков и систем программирования, соответствующих методов защиты информации, математического аппарата, других профессиональных знаний для решения поставленных в ВКР задач для разработки комплекса мер по обеспечению информационной безопасности объекта информатизации и организации их внедрения и последующего сопровождения . При защите информации ограниченного доступа организация технологического процесса защиты должна выполняться в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспертному контролю. В зависимости от вида определяемой темой ВКР деятельности (эксплуатационной, проектно-технологической, экспериментально – исследовательской или организационно-управленческой) данный этап прохождения практики конкретно включает: - завершение проектирования программных средств; - разработку и оформление политики безопасности информационной системы и (или) формирование разделов концепции защиты информации на объекте информатизации; - реализацию применения современных инструментальных средств разработки программно-аппаратного обеспечения, включая web-технологии; - оформление проектов организационно-распорядительных и методических документов и (или) рабочей технической документации с учетом действующих нормативных и методических документов; - разработку документационного обеспечения режима конфиденциальности информации; - технико-экономическое обоснование соответствующего проектного решения.
4.Экспериментальный {творческое задание} (18ч.)[1,2,3]	Разработка или выбор методики проведения аудита безопасности, эксперимента или иных мероприятий по оценке достоверности и качества полученных на предыдущем этапе результатов по проектированию, разработке, модернизации и исследованию средств обеспечения информационной безопасности. Применение выбранной или разработанной методики для

	проведения соответствующих экспериментальных исследований или иных мероприятий по проверке работоспособности и эффективности применения использованных в работе программных, программно-аппаратных и технических средств защиты информации, а если результатом ВКР является разработка технической документации – то проверки её на соответствие действующим нормативным актам. Обработка полученных в ходе исследования или проведенных мероприятий результатов, включающая, с целью установления оценку достоверности и/или оценку погрешности выполненных экспериментов (если только это возможно).
5.Пост – проектный {разработка проекта} (18ч.)[1,2,3]	Внедрение (если возможно) результатов работы или их передача в опытную эксплуатацию и организация контроля защищенности объекта информатизации при его последующем сопровождении в соответствии с нормативными документами. Оформление рабочей технической документации по результатам выполненных работ с учетом действующих нормативных и методических документов. Написание чернового варианта пояснительной записки к выпускной квалификационной работе.
6.Оформление и защита отчета по практике(18ч.)	

5. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

Для успешного освоения дисциплины используются ресурсы электронной информационно-образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное взаимодействие обучающегося с преподавателем через личный кабинет студента.

№пп	Используемое программное обеспечение
6	Chrome
9	Гарант
8	7-Zip
1	LibreOffice
7	Inkscape
2	Windows
3	Антивирус Kaspersky
5	GIMP
4	Foxit Reader

№пп	Используемые профессиональные базы данных и информационные справочные системы
1	IEEE Xplore - Интернет библиотека с доступом к реферативным и полнотекстовым статьям и материалам конференций. Бессрочно без подписки (https://ieeexplore.ieee.org/Xplore/home.jsp)
2	Springer - Издательство с доступом к реферативным и полнотекстовым материалам журналов и книг (https://www.springer.com/gp https://link.springer.com/)
3	Wiley - Издательство с доступом к реферативным и полнотекстовым материалам журналов и книг. Содержит большой раздел Computer Science & Information Technology, содержащий pdf-файлы с полными текстами журналов и книг издательства. Фиксируется пользователь информации на уровне вуза (Access byPolzunov Altai State Technical University) (https://www.wiley.com/en-ru https://www.onlinelibrary.wiley.com/)
4	Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам" для студентов и преподавателей; каталог ссылок на образовательные интернет-ресурсы (http://Window.edu.ru)
5	Национальная электронная библиотека (НЭБ) — свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог изданий, хранящихся в библиотеках России. (http://нэб.рф/)
6	Справочно-информационный портал ГРАМОТА.РУ (http://gramota.ru/)

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

а) основная литература

1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 13.02.2021). – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – Текст : электронный

2. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Санкт-Петербургский государственный политехнический университет. – Санкт-Петербург : Издательство Политехнического университета, 2014. – 322 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=363040 (дата обращения: 13.02.2021). – ISBN 978-5-7422-4331-1. – Текст : электронный

3. Малюк, А. А. Теория защиты информации / А. А. Малюк. — Москва : Горячая линия-Телеком, 2015. — 184 с. — ISBN 978-5-9912-0246-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111077 (дата обращения: 13.02.2021). — Режим доступа: для авториз. пользователей

б) дополнительная литература

4. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 13.02.2021). – Библиогр. в кн. – Текст : электронный

5. Технические средства и методы защиты информации : учебное пособие / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков, И. В. Голубятников. — Москва : Горячая линия-Телеком, 2012. — 616 с. — ISBN 978-5-9912-0084-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5154 (дата обращения: 13.02.2021). — Режим доступа: для авториз. пользователей

6. Основы управления информационной безопасностью. Серия «Вопросы управления информационной безопасностью". Выпуск 1 : учебное пособие / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 244 с. — ISBN 978-5-9912-0271-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5178 (дата обращения: 13.02.2021). — Режим доступа: для авториз. пользователей

в) ресурсы сети «Интернет»

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

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

9. Портал в области компьютерной безопасности. = URL: https://www.securitylab.ru/

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Учебные аудитории для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

При организации практики АлтГТУ или профильные организации предоставляют оборудование и технические средства обучения в объеме, позволяющем выполнять определенные виды работ, указанные в задании на практику.

Практика для обучающихся с ограниченными возможностями здоровья и инвалидов проводится с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

8. ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ

Оценка за практику выставляется на основе защиты студентами отчёта о практике.

Отчет о практике должен отражать результаты овладения универсальными и общепрофессиональными компетенциями и содержать титульный лист, индивидуальное задание, содержание, введение, состоящую из трех разделов основную часть, заключение, список использованных источников информации и (при необходимости) приложений.

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

Первый раздел включает 10-20 страниц. В нем дается описание предметной области исследований, анализ объекта (функционального процесса объекта) защиты информации (включая информационные потоки), описание и критический анализ аналогичных известных исследований, научно-исследовательских и технических разработок по защите объекта по теме ВКР, обоснование актуальности разработки, постановку цели и задач выпускной работы

Второй раздел включает 10-20 страниц и посвящен исследованиям уязвимости объекта и его

элементов, разработке модели угроз безопасности информации, расчёту рисков, определению требований к разрабатываемым подсистемам или средствам и проверку их на соответствие нормативно-правовым актам и стандартам, методическим документам ФСБ и ФСТЭК России и других регуляторов. Если ВКР связана с экспериментально – исследовательским видом деятельности, то в этом разделе описываются выбранные или разработанные методики экспериментальных исследований, алгоритмы обработки данных, структура создаваемого программно-технического комплекса или средства защиты, предлагаемые проектные решения и иные связанные с разработкой сведения.

Третий раздел включает 10-20 страниц и описывает комплексные решения по защите информации объекта информатизации или организации, состав и структуру организационно-распорядительных, методических, рабочих и технических документов, результаты экспериментальных исследований, испытаний и проверок разработанных методов, устройств и систем, предназначенных для обеспечения защиты информации. В зависимости от вида деятельности здесь могут также рассматриваться методики, технологии разработки структуры и содержания политик информационной безопасности, концепции 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 программного обеспечения, 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 выносятся листинги программ, проекты разработанных документов различного назначения (политики безопасности, концепции, положения, инструкции, технические паспорта и т.д.), иная дополнительная информация.

Общий объем отчета без учета приложений должен составлять не менее 40-45 страниц печатного текста. Конкретное содержание и структура отчета определяются тематикой ВКР и согласовываются с руководителем ВКР. В процессе подготовки отчета консультация с руководителем ВКР также обязательна. Перед защитой он просматривает уже готовый отчет и выставляет за него свою оценку. Эта оценка учитывается в итоговом рейтинге, выставляемом по результатам защиты.

При защите используется фонд оценочных материалов, содержащийся в программе практики. К промежуточной аттестации допускаются студенты, полностью выполнившие программу практики и представившие отчёт. Сдача отчета о практике осуществляется на последней неделе практики. Формой промежуточной аттестации по практике является зачёт с оценкой.

Студенты, не выполнившие программу практики, или не сдавшие и не защитившие отчёт, не допускаются к выполнению выпускной квалификационной работы.