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

УТВЕРЖДАЮ
Начальник УМУ АлтГТУ
_____ Н. П. Щербаков
"25" 04 2015 г.

Программа 3-ей учебной практики

Направление подготовки
«Информационная безопасность»

Квалификация (степень) выпускника
бакалавр

Барнаул 2015

1 Цели учебной практики

Целями учебной практики являются:

- закрепление у выпускников общекультурных и профессиональных компетенций, создание предпосылок самосовершенствования и профессионального роста личности;
- углубление теоретической подготовки в области эксплуатации компонентов систем комплексной защиты объектов информатизации, администрированию подсистем информационной безопасности объекта (АС и ИТКС), участие в проведении аттестации объектов информатизации (в том числе помещений) по требованиям безопасности информации;
- закрепление навыков по выполнению проектно- технологической деятельности, включающих анализ исходных данных для проектирования систем, проведение проектных расчетов элементов систем обеспечения информационной безопасности, участие в разработке технологической и эксплуатационной документации;
- закрепление навыков экспериментально - исследовательской деятельности, включающих сбор, изучение научно-технической информации, проведение экспериментов по заданной методике, обработка и анализ результатов, проведение вычислительных экспериментов с использованием стандартных программных средств;
- закрепление знаний, умений и навыков организационно – управленческой деятельности, включающих организацию работы малых коллективов исполнителей, организацию технологического процесса комплексной защиты информации объекта, разработку предложений по совершенствованию системы управления информационной безопасности.

2 Задачи учебной практики

Задачами учебной практики являются:

в области эксплуатационной деятельности:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;
- администрирование подсистем информационной безопасности объекта.

в области проектно-технологичесой деятельности:

- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;

- участие в разработке технологической и эксплуатационной документации;
- проведение предварительного технико-экономического обоснования проектных расчетов.

в области экспериментально-исследовательской деятельности:

- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств.

в области организационно-управленческой деятельности:

- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей с учетом требований защиты информации;
- совершенствование системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны;
- контроль эффективности реализации политики информационной безопасности объекта.

3 Место учебной практики в структуре основной образовательной программы

Учебная практика разбита на 3 части.

Третья часть учебной практики базируется на дисциплинах «Информатика» (1 семестр), «Основы информационной безопасности» (1 и 2 - ой семестр), «Языки программирования» (1 семестр), «Документоведение» (1 семестр), «Информационные процессы и системы» (2 семестр), «Теория информации» (3 семестр), «Организационное и правовое обеспечение информационной безопасности» (3, 4 семестры), «Технологии и методы программирования» (3 семестр), «Электротехника» (3 семестр), «Электроника и схемотехника» (4 семестр), «Основы WEB-технологий» (6, семестр), «Технические средства охраны» (5 семестр).

Третья часть учебной практики связана с разработкой индивидуального задания, связанного с темой будущей выпускной квалификационной работы. В связи с этим знания, умения и навыки, требующиеся студенту для выполнения задания по практике, связаны с тематикой ВКР.

В ходе практики знания, умения и навыки закрепляются и совершенствуются, кроме того студент может освоить новые программные и технические продукты в сфере информационной безопасности, вести информационное обслуживание производственной деятельности (при прохождении учебной практики на предприятии).

Результаты выполнения третьей части учебной практики используются в дисциплине «Информационная безопасность предприятия (организации)» (8 семестр), «Информационно-аналитическая деятельность по обеспечению комплексной безо-

пасности» (7 семестр), «Инженерно-техническая защита информации» (7 семестр), «Проверка информационной защищенности на соответствие нормативным документам» (7 семестр), «Информационная безопасность автоматизированных систем» (7 семестр), «Основы научных исследований» (8 семестр), «Системы видеоконтроля и контроля управления доступом» (8 семестр). «Основы научных исследований» (8 семестр), выполнении выпускной квалификационной работы.

4 Формы проведения учебной практики

Форма проведения практики – лабораторная для первой и второй частей практики (база практики ФГОБУ «Алтайский государственный технический университет им.И.И.Ползунова»), производства или отделы защиты информации – для третьей части практики, когда студент может выполнять задание по практике по заявке с предприятия-базы практики.

5 Место и время проведения учебной практики

Третья часть учебной практики база практики – ФГОБУ «Алтайский государственный технический университет им.И.И.Ползунова» или предприятие, в соответствии с договором на практику:

- отделы защиты информации государственных и коммерческих организаций г. Барнаула и Алтайского края;
- отделы защиты информации и информационные отделы органов государственной и муниципальной власти;
- организации, осуществляющие услуги в области защиты информации;
- информационные отделы государственных и коммерческих организаций;
- управление безопасности и отделения Сбербанка России, коммерческих банков;
- управления и отделы безопасности государственных и коммерческих организаций;
- структурные подразделения АлтГТУ.

Время проведения практики – 1-4 недели после летней сессии третьего курса.

6 Компетенции обучающегося, формируемые в результате прохождения учебной практики

В результате прохождения учебной практики обучающийся должен приобрести практические навыки, умения, общекультурные и профессиональные компетенции в соответствии с ФГОС ВПО и ООП.

Декомпозиция компетенций, знаний, умений и владений (навыков) приведена в таблице 6.1

Таблица 6.1

Номер/ индекс компетенции по ФГОС ВПО	Содержание компетенции	В результате практики обучающиеся должны:		
		знать	уметь	владеть
ОК-5	способность к копе-	- механизмы обще-	- выбирать пра-	-способностью к коопера-

	рации с коллегами, работе в коллективе	ния; - качества, необходимы для эффективного, бесконфликтного общения; - нравственно – этические ценности в процессе общения;	вильную стратегию и тактику в процессе общения с коллегами; - уметь предотвращать конфликты при работе в коллективе;	ции с коллегами - способностью работать в коллективе
ОК-6	способность находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность	-основные понятия и методы в области управленческой деятельности	-оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения	-навыками обоснования, выбора, реализации и контроля результатов управленческого решения.
ОК-7	способность осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства	-основные понятия экономической и финансовой деятельности отрасли и ее структурных подразделений; -основы: российской правовой системы и законодательства, правового статуса личности правовые основы обеспечения национальной безопасности Российской Федерации;	-анализировать мировоззренческие, социально и личностно значимые философские проблемы, анализировать и оценивать социальную информацию; -планировать и осуществлять свою деятельность с учетом результатов этого анализа;	- навыками самостоятельной работы, способностью принимать решения в рамках своей профессиональной компетенции;
ОК-8	способность к обобщению, анализу, восприятию инфомации, постановке цели и выбору путей ее достижения, владеть культурой мышления	- методы анализа информации; - способы достижения целей, поставленных в задании на прак-тику	- решать задачи обработки информации	-способностью к обобщению, анализу и восприятию информации; -навыками выбора путей решения задач обработки информации
ОК-9	способность логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять	- грамматику русского и иностранного языков, правила речевого этикета; - лексический минимум в объеме	- переводить профессиональные тексты на иностранном языке; -аргументированно устно и пись-	- иностранным языком в объеме, необходимом для возможности получения информации по профессиональной тематике, и навыками устной речи;

	собственные и известные научные результаты, вести дискуссии	4000 учебных лексических единиц общего и терминологического характера (для иностранного языка); - основные формы делового общения	менно излагать собственную точку зрения	- культурой речи и навыками грамотного письма
ОК-11	способность к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства	-методы повышения квалификации и мастерства	- применять методы и средства познания для интеллектуального развития, повышения культурного уровня, профессионального роста	- способностью к переоценке накопленного опыта, анализу своих возможностей, готовностью приобретать новые знания; - навыками саморазвития
ОК-12	способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков	-методы оценки достоинств и недостатков, выбора средств развития достоинств, устранения недостатков	-критически оценивать свои достоинства и недостатки, определять пути и выбирать средства развития достоинств и устранения недостатков	-навыками оценки своих достоинств и недостатков, определять пути и выбира средств развития достоинств и устранения недостатков
ПК-1	способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;	- основные естественнонаучные законы, - математический аппарат используемый в профессиональной деятельности, - сущность проблем, возникающих в ходе профессиональной деятельности;	-использовать математические методы и модели для решения прикладных задач; - применять основные законы физики при решении прикладных задач; - использовать программные и аппаратные средства персонального компьютера.	-методами количественного анализа процессов обработки, поиска и передачи информации; - навыками проведения физического эксперимента и обработки его результатов;
ПК-2	способность понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной	- общие принципы организации и функционирования вычислительных и информационных систем; - технологию работы в различных	- работать в локальных и глобальных компьютерных сетях; - работать с объектами файловой системы; - использовать	-навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средст-

	техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;	операционных и программных средах;	сетевые технологии для доступа к информационным ресурсам .	вами подготовки презентационных материалов, СУБД и т.п.).
ПК-3	способность использовать нормативные правовые документы в своей профессиональной деятельности	-основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;	- пользоваться нормативными документами по защите информации;	-навыками работы с нормативными правовыми актами;
ПК-4	способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	-место и роль информационной безопасности в системе национальной безопасности Российской Федерации;	- формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно управленческой и технической реализуемости и экономической целесообразности	-формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно управленческой и технической реализуемости и экономической целесообразности
ПК-5	способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с уче-	-комплекс мер по информационной безопасности, с учетом решаемых задач и организационной структуры объекта защиты, внешних воз-	-применять комплекс мер по информационной безопасности, с учетом решаемых задач и организационной структуры объекта защи-	-навыками применения комплекса мер по ИБ, с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты

	том решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации	действий, вероятных угроз	ты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации	информации
ПК-8	способность определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	-виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	-определять виды и формы информации, подверженной угрозам, виды и методы реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	-навыками определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия
ПК-9	способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия	-основы эксплуатации подсистем управления информационной безопасностью предприятия	-принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия	-навыки в эксплуатации подсистем управления информационной безопасностью предприятия
ПК-10	способностью администрировать подсистемы информационной безопасности объекта	- эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы;	- администрировать подсистемы информационной безопасности объекта	- методами администрирования подсистемы информационной безопасности объекта
ПК-11	способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств 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;	-осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;	- методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; - навыками выявления и уничтожения компьютерных вирусов; -методами технической защиты информации; - методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;

		- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;		
ПК-12	-способность участвовать в разработке подсистемы управления информационной безопасностью	-основы администрирования вычислительных сетей; аппаратные средства вычислительной техники;	- участвовать в разработке подсистемы управления информационной безопасностью - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;	- навыками участвовать в разработке подсистемы управления информационной безопасностью
ПК-13	способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности	- основы технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности	- проводить технико-экономический анализ и обоснование проектных решений по обеспечению ИБ	- методами анализа и формализации информационных процессов объекта и связей между ними;
ПК-14	способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности	- правила оформления рабочей технической документации с учетом действующих нормативных и методических документов в области информационной безопасности	- оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности	-навыками оформления рабочей технической документации с учетом действующих нормативных и методических документов в области информационной безопасности
ПК-15	способностью применять программные средства системного, прикладного и специального назначения	- методы программирования и методы разработки эффективных алгоритмов решения прикладных	- составлять, тестировать, отлаживать и оформлять программы на языках высокого	- методами тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;

		задач;	уровня, включая объектно-ориентированные;	
ПК-16	способностью использовать инструментальные средства и системы программирования для решения профессиональных задач	- современные средства разработки и анализа программного обеспечения на языках высокого уровня;	- выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах;	- методами выбора необходимых инструментальные средства для разработки программ в различных операционных системах и средах;
ПК-19	способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности	- порядок и правила составления обзора по вопросам обеспечения информационной безопасности	- составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности	- навыками составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности
ПК-20	способностью применять методы анализа изучаемых явлений, процессов и проектных решений	- методы анализа изучаемых явлений, процессов и проектных решений	- применять методы анализа изучаемых явлений, процессов и проектных решений	- навыками применять методы анализа изучаемых явлений, процессов и проектных решений
ПК-24	способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	- способы осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	- осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	- навыками подбора, изучения и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности
ПК-28	способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации	- принципы организации информационных систем в соответствии с требованиями по защите информации;	- изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации	-методами обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации
ПК-29	способность участвовать в работах по реализации политики информационной безопасности	- порядок разработки и реализации политики информационной безопасности	- участвовать в работах по реализации политики информационной безопасности	- навыками участия в работах по реализации политики информационной безопасности

ПК 30	способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности	- основы комплексного подхода к обеспечению информационной безопасности предприятия	применять комплексный подход к обеспечению ИБ в различных сферах деятельности	- навыками комплексного подхода к обеспечению ИБ в различных сферах деятельности
ПК-32	способность организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации (ПК-32);	- опасные и вредные факторы системы "человек - среда обитания", методы анализа антропогенных опасностей, научные и организационные основы защиты окружающей среды и ликвидации последствий, аварий, катастроф, стихийных бедствий.	- анализировать и оценивать степень риска проявления факторов опасности системы "человек - среда обитания", осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности.	- навыками безопасного использования технических средств в профессиональной деятельности.

7 Структура и содержание учебной практики

Общая трудоемкость учебной практики составляет 12 зачетных единиц, (432 часа).

Третья часть учебной практики – 216 часов (6 зачетных единиц)

В процессе прохождения третьей части учебной практики осуществляется выполнение следующих видов работ, связанных с темой будущей выпускной квалификационной работы:

- исследование уязвимости объектов защиты различного уровня и назначения;
- аудит безопасности объекта;
- разработка компонентов или элементов комплексной системы защиты информации объекта информатизации;

№ п/п	Разделы (этапы) практики	Виды учебной работы на практике, включая СРС и их трудоемкость в часах	Формы текущего контроля
1	2	3	4
1	Инструктаж по технике безопасности	2	Запись в журнале инструктажа
1	2	3	4
2	Исследование уязвимости объектов защиты различного уровня и назначения, аудит безопасности	200	Представление руководителю практики отчёта

	объекта, разработка компонентов или элементов комплексной системы защиты информации объекта информатизации (согласно варианту задания)		
3	Подготовка отчета по практике	16	Защита

8 Образовательные, научно-исследовательские и научно-производственные технологии, используемые на учебной практике

При прохождении учебной практики используются следующие технологии:

- технология поиска и отбора информации;
- технология развития критического мышления.
- интернет-технологии;
- сетевые технологии;
- технологии использования программно-технического обеспечения;
- технологии электронного обучения;
- технология мастер-классов;
- технология проектной деятельности;
- 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 учебной практике

Студент получает задание на практику (см. приложение Б), и, необходимую документацию для выполнения задания.

Для второй части практики студент должен демонстрировать преподавателю не реже, чем раз в пять календарных дней результаты разработки и реализации политики безопасности.

Задания по практике, выполняются студентом самостоятельно и индивидуально. В течение практики студент консультируется у руководителя практики, у специалистов предприятия-базы практики.

В заключительной части отчета о практике студент должен проявить компетенции, сформированные при выполнении задания.

Отчет о практике студент защищает в комиссии, назначаемой заведующим кафедрой, в состав которой может входить представитель базы практики.

Контрольные вопросы при защите практики задаются по теме практики и являются индивидуальными для каждой темы и каждого студента. Примеры тем первой части учебной практики приведены в приложении В. По второй части практики контрольные вопросы задаются только по разработанному программному продукту.

Оценка по практике проставляется в соответствии с Положением о модульно-рейтинговой системе квалиметрии учебной деятельности студентов, приравнивается

к оценкам по теоретическому обучению и учитывается при подведении итогов общей успеваемости студентов.

10 Формы промежуточной аттестации (по итогам практики)

По окончании каждой части учебной практики студент составляет письменный отчет и сдает его в десятидневный срок руководителю практики от университета вместе с календарным планом. Календарный план подписывается для первой и второй части руководителем от вуза, для третьей части - научным руководителем, который является руководителем практики от организации.

Студенты, не выполнившие программы практики по уважительной причине, направляются на практику вторично, в свободное от учебы время.

Отчет о практике оформляет каждый студент независимо от вида задания.

Отчет о практике должен содержать:

- титульный лист, оформленный согласно приложению А;
- задание и календарный план выполнения практики, подписанные руководителем практики, оформленный согласно приложению Б;
- введение;
- анализ выполненной работы;
- заключение;
- источники информации;
- приложения.

Введение должно содержать общие сведения о практике и краткую характеристику базы практики (для третьей части учебной практики).

Раздел “Анализ выполненной работы” является основной частью отчета и составляет примерно 90% его объема. В разделе дается описание и анализ выполненной работы с количественными и качественными характеристиками ее элементов. Приводятся необходимые иллюстрации.

В разделе “Заключение” студент должен:

- кратко изложить состояние и перспективы развития изученных на практике систем (объектов, процессов);
- отметить недостатки действующей системы и конкретные пути ее улучшения и замены;
- проявить универсальные и профессиональные компетенции.

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, СТП 12 570-2006 СТАНДАРТ ПРЕДПРИЯТИЯ. Система менеджмента качества. Образовательный стандарт высшего профессионального образования АлтГТУ. ОБЩИЕ ТРЕБОВАНИЯ К ТЕКСТОВЫМ, ГРАФИЧЕСКИМ И ПРОГРАММНЫМ ДОКУМЕНТАМ .

Общий объем отчета по первой части учебной практики должен соответствовать 20-40 страницам печатного текста, для второй части – 10-15 страниц, для третьей части – 15-30 страниц.

11 Учебно-методическое и информационное обеспечение учебной практики

а) основная литература – из СТП учебных дисциплин пререквизитов соответствующего раздела учебной практики

б) дополнительная литература - из СТП учебных дисциплин пререквизитов соответствующего раздела учебной практики

в) программное обеспечение и Интернет-ресурсы

1 www.google.com
2 www.edu.ru
3 www.edulib.ru,
4 www.intuit.ru
5 Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [электронный ресурс]:- режим доступа: http:// www.fstec.ru.
6 Официальный сайт федерального агентства по техническому регулированию и метрологии [электронный ресурс]: режим доступа: http://protect.gost.ru//
7 Правовая справочная система «Гарант» [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ.(Платформа F1 Гарант); 2. http://www.garant.ru
8 интернет-источники с технической литературой, документацией на программы, аппаратные устройства, сети, системы

12 Материально-техническое обеспечение учебной практики

Для проведения учебной практики используются компьютерные классы и лаборатории кафедры ИВТиИБ, а также учебно-лабораторная и производственная база предприятий-баз практики. Учебно-лабораторный комплекс кафедры базируется на лаборатории электронной, микропроцессорной, вычислительной и специальной техники, центре «Медицина и электроника», межкафедральной лаборатории информационно-измерительных систем, лаборатории сетевого программного обеспечения и защиты информации в компьютерных сетях, лаборатории комплексных систем защиты информации, лаборатории микро-ЭВМ.

Автор(ы) _____ Ю.Н. Загинайлов, профессор каф. ИВТиИБ
(подпись) (ИОФ, должность, кафедра)

_____ Е.В. Шарлаев, доцент каф. ИВТиИБ
(подпись) (ИОФ, должность, кафедра)

Программа рассмотрена и одобрена на заседании кафедры
«Информатика, вычислительная техника и информационная безопасность»
(наименование кафедры)

«22» 04 2015 г., протокол № 8

Заведующий кафедрой _____ А.Г. Якунин
(подпись) (ИОФ)

Программа рассмотрена и одобрена на заседании
Совета факультета информационных технологий
(наименование факультета)

«22» 04 2015 г., протокол № 7

Председатель Совета (декан ФИТ) _____ Е.А. Зрюмов
(подпись) (ИОФ)

Согласовано:

И.о. начальника отдела практик
и трудоустройства _____ И.Г. Таран
(подпись) (ИОФ)

«20» 04 2015 г.

Лист внесения изменений

ИЗМЕНЕНИЕ (ДОПОЛНЕНИЕ) № 1

Дата введения <2015-04-22>

Утверждено и введено в действие Протоколом заседания кафедры «Информатика, вычислительная техника и информационная безопасность»

от 22 апреля 2015 г. № 8

Внесены следующие изменения в программу 3-ей учебной практики:

1. В связи с приказом Д-65 от 24.03.2014 г. об объединении кафедр ВСИБ и САПР и присвоении новой кафедре названия «Информатика, вычислительная техника и информационная безопасность» (ИВТ и ИБ) заменить название кафедры «Вычислительные системы и информационная безопасность» на название «Информатика, вычислительная техника и информационная безопасность». Заменить аббревиатуру ВСИБ на аббревиатуру ИВТ и ИБ.
2. Введено приложение В Фонд оценочных средств.

3. В связи с приказом Минобрнауки России №270 от 25.03.2015 г. заменить шифр 090900 направления Информационная безопасность на шифр 10.03.01.

ПРИЛОЖЕНИЕ А
Форма титульного листа отчета о практике

Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
”Алтайский государственный технический университет им. И. И. Ползунова”

Факультет информационных технологий

Кафедра информатики, вычислительной техники и информационной безопасности

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

ОТЧЕТ

О 3-ей учебной практике

в _____
наименование организации

Студент гр. ИБ-11_____Иванов А.В._____

индекс группы *подпись* *Ф. И. О.*

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

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

20__

ПРИЛОЖЕНИЕ Б

Форма задания и календарного плана практики

ФГБОУ ВО “Алтайский государственный технический университет им. И. И. Ползунова”

Кафедра информатики, вычислительной техники и информационной безопасности

УТВЕРЖДАЮ

Зав. кафедрой_____А. Г. Якунин

“____”_____20___г.

ЗАДАНИЕ

По 3-ей учебной практике

студенту группы ИБ-11

_____

фамилия, имя, отчество

__10.03.01 Информационная безопасность___

код и наименование направления

База практики_____

наименование организации

Срок практики с _____20__г. по _____20____г.

_____

общая формулировка задания

Календарный план практики

Наименование задач (мероприятий), составляющих задание	Дата выполнения задачи (мероприятия)	Подпись руководителя практики от организации
1	2	3

Срок представления отчёта к защите_____

Руководитель практики от вуза

_____

подпись *Ф. И. О., должность*

ПРИЛОЖЕНИЕ В

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ТРЕТЬЕЙ УЧЕБНОЙ ПРАКТИКЕ

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

Код контролируемой компетенции	**Этап формирования компетенции**	**Способ оценивания**	**Оценочное средство**
ОК-5 способность к копе-рации с коллегами, работе в коллективе	итоговый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ОК-6 способность находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность	итоговый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ОК-7 способность осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства	итоговый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ОК-8 способность к обобщению, анализу, восприятию инфома-ции, постановке цели и выбору путей ее достижения, владеть культурой мышления	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ОК-9 способность логии-чески верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ОК-11 способность к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ОК-12 способностью критически оценивать свои достоинства и недостатки, определять пути	базовый	Анализ отчета по практике, за-	Комплект контролирующих материалов и иных заданий для за-

и выбрать средства развития достоинств и устранения недостатков		щита	щиты отчёта о практике
ПК-1 способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-2 способность понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-3 способность использовать нормативные правовые документы в своей профессиональной деятельности	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-4 способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-5 способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-8 способность определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реа-	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике

лизации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия			
ПК-9 способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-10 способностью администрировать подсистемы информационной безопасности объекта	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-11 способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-12 способность участвовать в разработке подсистемы управления информационной безопасностью	начальный	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-13 способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-14 способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-15 способностью применять программные средства системного, прикладного и специального назначения	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-16 способностью использовать инструментальные средства и системы программирования для решения профессиональных задач	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-19 способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-20 способностью применять	базовый	Анализ отчета	Комплект контроли-

методы анализа изучаемых явлений, процессов и проектных решений		по практике, защита	рующих материалов и иных заданий для защиты отчёта о практике
ПК-24 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-28 способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-29 способность участвовать в работах по реализации политики информационной безопасности	начальный	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК 30 способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности	начальный	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике
ПК-32 способность организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации (ПК-32)	базовый	Анализ отчета по практике, защита	Комплект контролирующих материалов и иных заданий для защиты отчёта о практике

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

Показатели оценивания компетенций представлены в разделе «Компетенции обучающегося, формируемые в результате прохождения практики» программы третьей учебной практики с декомпозицией: знать, уметь, владеть.

При оценивании сформированности компетенций по первой учебной практике используется 100-балльная шкала.

Критерий	**Оценка по 100-балльной шкале**	
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 положи-	75-100	*Отлично*

тельный отзыв от руководителя практики. Отчет в полном объеме соответствует заданию на практику.		
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*

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

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

1. Какие способы решения задачи, поставленной Вам на период практики, известны?
2. Применительно к какому компоненту системы защиты информации вы проводили исследование?
3. Какие новые программно-аппаратные средства Вы изучили?
4. Какие новые технические средства защиты вы изучили?
5. Какие новые средства оценки эффективности защиты вы изучили?
6. Какие новые нормативные и нормативно-методические документы ФСБ РФ и ФСТЭК РФ вы изучили?
7. Какие нормативные документы вы разработали лично, в разработке каких участвовали?
8. Какая аппаратная база использовалась Вами в период практики?
9. Дайте краткую характеристику изученных машин, комплексов, систем и сетей предприятия.
10. Какую информацию Вы собрали и проанализировали за период практики?
11. Какие направления разработки программного обеспечения Вы выбрали для дальнейшей работы?

12. Вы участвовали в работах по наладке, настройке и опытной проверке оборудования, вычислительных сетей?

13. Вы участвовали в работах по инсталляции, настройке и опытной проверке программных средств защиты?

14. Какие среды разработки ПО Вы изучили?

15. Какие сайты профессиональной направленности Вы периодически посещаете?

16. Какие инструменты поиска информации в глобальных сетях Вы знаете?

17. С какими операционными системами Вы знакомы?

18. Какие источники информации Вы использовали при подготовке отчета по практике? Почему именно эти?

19. Вы считаете полученные за время практики результаты значительными? Почему?

20. Вы успешно входите в новый коллектив? Почему вы так считаете?

21. Вы проявили себя хорошим работником за время практики? Почему вы так думаете?

22. Проводилась ли Вами работа по анализу экспериментальных данных?

23. Оцените, какие факторы влияли на успешность Вашей работы в период практики?

24. Проводилась ли работа с базами данных?

25. Какие интерфейсные решения Вы изучили за период практики? В чем их достоинства и недостатки?

26. Что нового Вы узнали в период практики, как это повлияло на Ваши профессиональные предпочтения?

27. Как обеспечивалась в период практики охрана труда и выполнялась техника безопасности? Каково положение с этим вопросом на предприятии?

4. 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 сведения, СТО АлтГТУ 12330-2014 Практика. Общие требования к организации, проведению и программе практики и СМК ОПД-01-19-2008 Положение о модульно-рейтинговой системе квалиметрии учебной деятельности студентов, а также соответствующими разделами стандарта настоящей дисциплины.

Практические задания:

ПЗ №1

В государственном учреждении обрабатываются, хранятся, передаются и представляются в вышестоящие органы сведения, составляющие государственную тайну. Для автоматизированной обработки этих сведений планируется использовать два автоматизированных рабочих места на базе персональных компьютеров расположенных в соседних помещениях. Для обсуждения секретных научных и технологических проблем планируется использовать отдельное помещение.

Определить:

1. Какие подсистемы должна иметь КСЗИП.

2.Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №2

В государственном учреждении обрабатываются, хранятся, передаются и представляются в вышестоящие органы сведения, составляющие служебную тайну. Для автоматизированной обработки этих сведений планируется использовать три автоматизированных рабочих места на базе персональных компьютеров объединённых в локальную сеть, расположенных в одном помещении.

Определить:

1. Какие подсистемы должна иметь КСЗИП.

2. Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №3

В коммерческой организации обрабатывается, хранится, передаётся и представляется в органы государственной власти и муниципальные органы информация, составляющая коммерческую тайну. Для автоматизированной обработки этих сведений планируется использовать семь автоматизированных рабочих мест на базе персональных компьютеров объединённых в локальную сеть, расположенных в разных помещениях. Для обсуждения коммерческих секретов планируется использовать отдельное помещение.

Определить:

1. Какие подсистемы должна иметь КСЗИП.

3. Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №4

В организации с негосударственной формой собственности имеется информационная система персональных данных (ИСПДн). По требованиям нормативных документов органов уполномоченных в области безопасности и технической защиты информации и противодействия техническим разведкам требуется обязательная аттестация ИСПДн по требованиям безопасности информации.

Определить:

1. Какие подсистемы должна иметь КСЗИП.

2.Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №5 На персональном компьютере должностного лица государственного учреждения, допущенного к государственной тайне по второй форме допуска, планируется обработка сведений, составляющих государственную тайну с грифом «Совершенно секретно» и «секретно». Предполагается, что он будет единственным пользователем АС.

Определить:

1. Какому классу должна соответствовать АС в соответствии с требованиями Руководящих документов, для аттестации её по требованиям безопасности.

2. Какому классу должна соответствовать ОС и (или) программно-аппаратные средства защиты (СВТ), для того чтобы обеспечить требуемый класс АС.

3. Какому классу должна соответствовать АС по уровню контроля недекларированных возможностей.

4. Какому классу должны соответствовать средства антивирусной защиты.

ПЗ №6 В локальной вычислительной сети отдела менеджеров коммерческой организации, состоящей из 5 персональных компьютеров хранятся и обрабатываются наряду с общедоступными, информационные ресурсы включающие информацию, составляющую **коммерческую тайну**. Локальная сеть интегрирована в корпоративную сеть организации, которая имеет выход в сеть Интернет. Условия обработки информации в отделе менеджеров: режим обработки – коллективный, уровень полномочий – различные права доступа.

Определить:

1. Какому классу должна соответствовать АС в соответствии с требованиями Руководящих документов, для аттестации её по требованиям безопасности.

2. Какому классу должна соответствовать СВТ (ОС и программно-аппаратные средства защиты, для того чтобы обеспечить требуемый класс АС.

3. Каким классам должны соответствовать средства антивирусной защиты на сервере и рабочих станциях сети.

4. Какому классу должен соответствовать межсетевой экран.

ПЗ №7 В локальной вычислительной сети отдела документационного обеспечения государственного учреждения, состоящей из 3 персональных компьютеров хранятся и обрабатываются наряду с общедоступными, информационные ресурсы включающие информацию для служебного пользования. Локальная сеть интегрирована в сеть организации, которая не имеет выхода в сети

общего пользования. Условия обработки информации в отделе: режим обработки – коллективный, уровень полномочий – одинаковые права доступа ко всей информации.

Определить:

1.Какому классу должна соответствовать АС в соответствии с требованиями Руководящих документов, для аттестации её по требованиям безопасности.

2.Какому классу должны соответствовать СВТ (ОС и программно-аппаратные средства защиты (СВТ), для того чтобы обеспечить требуемый класс АС.

3.Каким классам должны соответствовать средства антивирусной защиты на сервере и рабочих станциях сети.

4.Какому классу должен соответствовать межсетевой экран.

ПЗ №8

В государственном учреждении обрабатываются, хранятся, передаются и представляются в вышестоящие органы сведения, составляющие государственную тайну. Для автоматизированной обработки этих сведений планируется использовать два автоматизированных рабочих места на базе персональных компьютеров расположенных в соседних помещениях. Для обсуждения секретных научных и технологических проблем планируется использовать отдельное помещение.

Определить:

1. Какие подсистемы должна иметь КСЗИП.

2.Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №9

В государственном учреждении обрабатываются, хранятся, передаются и представляются в вышестоящие органы сведения, составляющие служебную тайну. Для автоматизированной обработки этих сведений планируется использовать три автоматизированных рабочих места на базе персональных компьютеров объединённых в локальную сеть, расположенных в одном помещении.

Определить:

1.Какие подсистемы должна иметь КСЗИП.

2.Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №10

В коммерческой организации обрабатывается, хранится, передаётся и представляется в органы государственной власти и муниципальные органы информация, составляющая коммерческую тайну. Для автоматизированной обработки этих сведений планируется использовать семь автоматизированных рабочих мест на базе персональных компьютеров объединённых в локальную сеть, расположенных в разных помещениях. Для обсуждения коммерческих секретов планируется использовать отдельное помещение.

Определить:

1.Какие подсистемы должна иметь КСЗИП.

2.Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №11

В организации с негосударственной формой собственности имеется информационная система персональных данных (ИСПДн). По требованиям нормативных документов органов уполномоченных в области безопасности и технической защиты информации и противодействия техническим разведкам требуется обязательная аттестация ИСПДн по требованиям безопасности информации.

Определить:

1. Какие подсистемы должна иметь КСЗИП.

2.Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №12 На персональном компьютере должностного лица государственного учреждения, допущенного к государственной тайне по второй форме допуска, планируется обработка сведений, составляющих государственную тайну с грифом «Совершенно секретно» и «секретно». Предполагается, что он будет единственным пользователем АС.

Определить:

1.Какому классу должна соответствовать АС в соответствии с требованиями Руководящих документов, для аттестации её по требованиям безопасности.

2.Какому классу должна соответствовать ОС и (или) программно-аппаратные средства защиты (СВТ), для того чтобы обеспечить требуемый класс АС.

3.Какому классу должна соответствовать АС по уровню контроля недекларированных возможностей.

4.Какому классу должны соответствовать средства антивирусной защиты.

ПЗ №13 В локальной вычислительной сети отдела менеджеров коммерческой организации, состоящей из 5 персональных компьютеров хранятся и обрабатываются наряду с общедоступными, информационные ресурсы включающие информацию, составляющую **коммерческую тайну**. Локальная сеть интегрирована в корпоративную сеть организации, которая имеет выход в сеть Интернет. Условия обработки информации в отделе менеджеров: режим обработки – коллективный, уровень полномочий – различные права доступа.

Определить:

1.Какому классу должна соответствовать АС в соответствии с требованиями Руководящих документов, для аттестации её по требованиям безопасности.

2.Какому классу должна соответствовать СВТ (ОС и программно-аппаратные средства защиты, для того чтобы обеспечить требуемый класс АС.

3.Каким классам должны соответствовать средства антивирусной защиты на сервере и рабочих станциях сети.

4.Какому классу должен соответствовать межсетевой экран.

ПЗ №14 В локальной вычислительной сети отдела документационного обеспечения государственного учреждения, состоящей из 3 персональных компьютеров хранятся и обрабатываются наряду с общедоступными, информационные ресурсы включающие информацию для служебного пользования. Локальная сеть интегрирована в сеть организации, которая не имеет выхода в сети общего пользования. Условия обработки информации в отделе: режим обработки – коллективный, уровень полномочий – одинаковые права доступа ко всей информации.

Определить:

1.Какому классу должна соответствовать АС в соответствии с требованиями Руководящих документов, для аттестации её по требованиям безопасности.

2.Какому классу должны соответствовать СВТ (ОС и программно-аппаратные средства защиты (СВТ), для того чтобы обеспечить требуемый класс АС.

3.Каким классам должны соответствовать средства антивирусной защиты на сервере и рабочих станциях сети.

4.Какому классу должен соответствовать межсетевой экран.

ПЗ №15

В государственном учреждении обрабатываются, хранятся, передаются и представляются в вышестоящие органы сведения, составляющие государственную тайну. Для автоматизированной обработки этих сведений планируется использовать два автоматизированных рабочих места на базе персональных компьютеров расположенных в соседних помещениях. Для обсуждения секретных научных и технологических проблем планируется использовать отдельное помещение.

Определить:

1. Какие подсистемы должна иметь КСЗИП.

2.Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №16

В государственном учреждении обрабатываются, хранятся, передаются и представляют-

ся в вышестоящие органы сведения, составляющие служебную тайну. Для автоматизированной обработки этих сведений планируется использовать три автоматизированных рабочих места на базе персональных компьютеров объединённых в локальную сеть, расположенных в одном помещении.

Определить:

1.Какие подсистемы должна иметь КСЗИП.

2.Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №17

В коммерческой организации обрабатывается, хранится, передаётся и представляется в органы государственной власти и муниципальные органы информация, составляющая коммерческую тайну. Для автоматизированной обработки этих сведений планируется использовать семь автоматизированных рабочих мест на базе персональных компьютеров объединённых в локальную сеть, расположенных в разных помещениях. Для обсуждения коммерческих секретов планируется использовать отдельное помещение.

Определить:

1. Какие подсистемы должна иметь КСЗИП.

2. Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №18

В организации с негосударственной формой собственности имеется информационная система персональных данных (ИСПДн). По требованиям нормативных документов органов уполномоченных в области безопасности и технической защиты информации и противодействия техническим разведкам требуется обязательная аттестация ИСПДн по требованиям безопасности информации.

Определить:

1. Какие подсистемы должна иметь КСЗИП.

2.Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №19 На персональном компьютере должностного лица государственного учреждения, допущенного к государственной тайне по второй форме допуска, планируется обработка сведений, составляющих государственную тайну с грифом «Совершенно секретно» и «секретно». Предполагается, что он будет единственным пользователем АС.

Определить:

1.Какому классу должна соответствовать АС в соответствии с требованиями Руководящих документов, для аттестации её по требованиям безопасности.

2.Какому классу должна соответствовать ОС и (или) программно-аппаратные средства защиты (СВТ), для того чтобы обеспечить требуемый класс АС.

3.Какому классу должна соответствовать АС по уровню контроля недекларированных возможностей.

4.Какому классу должны соответствовать средства антивирусной защиты.

ПЗ №20 В локальной вычислительной сети отдела менеджеров коммерческой организации, состоящей из 5 персональных компьютеров хранятся и обрабатываются наряду с общедоступными, информационные ресурсы включающие информацию, составляющую **коммерческую тайну**. Локальная сеть интегрирована в корпоративную сеть организации, которая имеет выход в сеть Интернет. Условия обработки информации в отделе менеджеров: режим обработки – коллективный, уровень полномочий – различные права доступа.

Определить:

1.Какому классу должна соответствовать АС в соответствии с требованиями Руководящих документов, для аттестации её по требованиям безопасности.

2.Какому классу должна соответствовать СВТ (ОС и программно-аппаратные средства защиты, для того чтобы обеспечить требуемый класс АС.

3.Каким классам должны соответствовать средства антивирусной защиты на сервере и ра-

бочих станциях сети.

4.Какому классу должен соответствовать межсетевой экран.

ПЗ №21 В локальной вычислительной сети отдела документационного обеспечения государственного учреждения, состоящей из 3 персональных компьютеров хранятся и обрабатываются наряду с общедоступными, информационные ресурсы включающие информацию для служебного пользования. Локальная сеть интегрирована в сеть организации, которая не имеет выхода в сети общего пользования. Условия обработки информации в отделе: режим обработки – коллективный, уровень полномочий – одинаковые права доступа ко всей информации.

Определить:

1.Какому классу должна соответствовать АС в соответствии с требованиями Руководящих документов, для аттестации её по требованиям безопасности.

2.Какому классу должны соответствовать СВТ (ОС и программно-аппаратные средства защиты (СВТ), для того чтобы обеспечить требуемый класс АС.

3.Каким классам должны соответствовать средства антивирусной защиты на сервере и рабочих станциях сети.

4.Какому классу должен соответствовать межсетевой экран.

ПЗ №22

В государственном учреждении обрабатываются, хранятся, передаются и представляются в вышестоящие органы сведения, составляющие государственную тайну. Для автоматизированной обработки этих сведений планируется использовать два автоматизированных рабочих места на базе персональных компьютеров расположенных в соседних помещениях. Для обсуждения секретных научных и технологических проблем планируется использовать отдельное помещение.

Определить:

1. Какие подсистемы должна иметь КСЗИП.

2.Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №23

В государственном учреждении обрабатываются, хранятся, передаются и представляются в вышестоящие органы сведения, составляющие служебную тайну. Для автоматизированной обработки этих сведений планируется использовать три автоматизированных рабочих места на базе персональных компьютеров объединённых в локальную сеть, расположенных в одном помещении.

Определить:

1. Какие подсистемы должна иметь КСЗИП.

2. Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №24

В коммерческой организации обрабатывается, хранится, передаётся и представляется в органы государственной власти и муниципальные органы информация, составляющая коммерческую тайну. Для автоматизированной обработки этих сведений планируется использовать семь автоматизированных рабочих мест на базе персональных компьютеров объединённых в локальную сеть, расположенных в разных помещениях. Для обсуждения коммерческих секретов планируется использовать отдельное помещение.

Определить:

1.Какие подсистемы должна иметь КСЗИП.

2.Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

ПЗ №25

В организации с негосударственной формой собственности имеется информационная система персональных данных (ИСПДн). По требованиям нормативных документов органов уполномоченных в области безопасности и технической защиты информации и противодействия техническим разведкам требуется обязательная аттестация ИСПДн по требованиям безопасности ин-

формации.

Определить:

1. Какие подсистемы должна иметь КСЗИП.

2.Какие основные нормативные документы должны использоваться для определения требований по защите информации для каждой подсистемы.

Тестовые вопросы

ИТЗИ

1. Какие существуют основные виды разведок?
2. В чем назначение и каковы функции видов разведки?
3. Что такое канал утечки информации?
4. Что такое прямой акустический канал утечки информации?
5. Чем характеризуется параметрический канал утечки информации?
6. Каковы основные направления оптической разведки?
7. Какие группы средств оптического наблюдения Вам известны?
8. Каковы основные показатели средств оптической разведки?
9. Чем характеризуются оптико-механические приборы визуального наблюдения?
10. В чем преимущество перископических систем визуального наблюдения?
11. Что такое фокусное расстояние объектива?
12. В чем преимущества и недостатки длиннофокусной оптики?
13. Каковы особенности использования короткофокусной оптики?
14. Каковы возможности современных средств радиоэлектронной разведки?
15. Какие Вам известны средства активной радиоэлектронной разведки?
16. В чем отличие активных и пассивных средств радиоэлектронной разведки?
17. Каковы функции технических средств акустической разведки?
18. В чем преимущества лазерных средств аудиального контроля?
19. Какие преимущества при акустической разведке дает применение стетоскопов?
20. Дайте классификацию средств акустической разведки с каналом передачи в радиочастотном диапазоне.
21. Чем отличаются активные, пассивные и полуактивные радиозакладки?
22. В чем преимущество средств акустической разведки с проводным каналом?
23. В чем преимущества использования направленных микрофонов бля акустической разведки?
24. Что такое акустические антенны?
25. Что такое направленный микрофон?
26. Каковы достоинства и недостатки суммирующего параболического микрофона?

ИБАС

1. Классификация способов НСД к информации по непосредственному объекту атаки.
2. Перечислите пять основных способов атак.
3. Обобщенный алгоритм подготовки и реализации атак на компьютерную информацию и КС.
4. Суть и цель атаки типа «Летучая смерть».
5. Понятие «конфиденциальности (секретности) информации»;
6. Атаки на сменные элементы системы защиты информации в КС.
7. Классификация удаленных атак.
8. Определение политики безопасности и дискреционного управления доступом Объективные внутренние источники угроз безопасности информации на объекте информатизации.
9. Перечислите группы требований к средствам защиты информации реализуемым в СВТ.
10. Дайте характеристику 3-й группе АС.
11. Определение модели безопасности и мандатного управления доступом.
12. Перечислите требования по защите информации от НСД для АС.

13. Дайте характеристику 2-й группе АС
14. Определение (сущность) диспетчера доступа (монитора обращений).
15. Назовите основные этапы классификации АС.
16. Дайте характеристику 3-й группе АС.
17. Понятие профиля защиты
18. Характеристика класса функциональных требований «FIA - идентификация/аутентификация».
19. Характеристика класса требований доверия безопасности «ACM-Управление Конфигурацией»
20. Понятие задания по безопасности.
21. Характеристика класса функциональных требований «FAU - аудит безопасности».
22. Характеристика класса требований доверия безопасности «ADO-Поставка и Действие».
23. Понятие функционального пакета.
24. Характеристика класса функциональных требований «FRU - использование ресурсов».
25. Характеристика класса требований доверия безопасности «ADV-Разработка».