Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Кафедра информатики и защиты информации

ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И РАДИОЭЛЕКТРОНИКИ
(Наименование института, факультета)

УТВЕРЖДАЮ

Заведующий кафедрой
Информатики и защиты информации

_____М.Ю. Монахов
"28" 09 2017 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ
(Наименование практики)

Направление подготовки
10.03.01 «Информационная безопасность»

Профиль (программа) подготовки
«Комплексная защита объектов информатизации»

Квалификация (степень) выпускника
Бакалавр

г. Владимир 2017

ВВЕДЕНИЕ

Практика – это часть основной образовательной программы высшего образования, обеспечивающая усвоение конкретных навыков в данной предметной области.

Производственная практика проводится в три этапа во время обучения.

1. Производственная практика по окончании 4 семестра обучения. Данная практика является стационарной и проводится в течение 2 недель в сторонних организациях (учреждениях, предприятиях) и структурных подразделениях по профилю направления информационной безопасности или на выпускающей кафедре и в научных лабораториях ВлГУ. Практика может быть выездной, если между кафедрой и организацией, принимающей студентов на практику заключен договор о направлении студентов на практику, решены все вопросы финансового обеспечения прохождения практики (в т.ч. расходы на проживание и проезд до места проведения практики). Кроме того, предприятие (организация) должна иметь достаточную материально-техническую базу, соответствующий профиль деятельности и квалифицированных специалистов в области защиты информации.

2. Производственная практика во время 6 семестра обучения. Данная практика является распределенной, параллельно с учебным процессом, стационарной и проводится в течение 1 и 1/3 недели на выпускающей кафедре и в научных лабораториях ВлГУ.

3. Производственная практика по окончании 6 семестра обучения. Данная практика является стационарной и проводится в течение 2 и 2/3 недели в сторонних организациях (учреждениях, предприятиях) и структурных подразделениях по профилю направления информационной безопасности или на выпускающей кафедре и в научных лабораториях ВлГУ.

Производственная практика проводится как непрерывно с выделением в учебном графике периода времени по окончании второго семестра обучения. Форма проведения является заводской или лабораторной. При прохождении практики на выпускающей кафедре и в научных лабораториях ВлГУ, руководство организационными аспектами производственной практики осуществляет преподаватель выпускающей кафедры информатики и защиты информации, назначаемый заведующим кафедрой ИЗИ. При прохождении практики на предприятиях и организациях, руководство организационными аспектами производственной практики осуществляет как преподаватель выпускающей кафедры, так и должностное лицо, назначаемое руководителем организации, принимающей студентов на практику (руководитель от предприятия).

В случае прохождения производственной практики в сторонней организации сотрудник этой организации может являться консультантом студента. В этом случае на кафедру должно быть представлено письмо, заверенное печатью организации, о согласии принять студента на практику с указанием фамилии, имени, отчества (полностью) и должности консультанта, его контактного телефона и адреса электронной почты. Вместо письма допускается иметь долгосрочный договор с организацией о сотрудничестве и всю информацию о руководителе от предприятия заполнять в дневнике практики.

Преподаватель осуществляет руководство содержательными аспектами практики, предоставляет бакалавру информацию по заданию на практику и осуществляет текущий контроль работы бакалавра. Обучаемые получают индивидуальное задание. Тема задания практики должна соответствовать профилю направления обучения и быть увязана с перечнем рекомендованных направлений выпускных квалификационных работ (дипломных работ), который ежегодно разрабатывается кафедрой в соответствии с профилем ее учебно-методической и научно-исследовательской деятельности. Тема задания производственной практики предлагается студентом по согласованию с научным руководителем соответствующего направления. Научным руководителем производственной практики может быть только преподаватель выпускающей кафедры.

Кроме индивидуального задания и в зависимости от тематики задания руководителя практики, при прохождении производственной практики студент должен:

Изучить:

- организацию и управление деятельностью по защите информации в организации;
- вопросы производимой, разрабатываемой или используемой техники, формы и методы сбыта продукции или предоставления услуг;
- действующие стандарты, технические условия, должностные обязанности, положения и инструкции по обеспечению информационной безопасности в организации, используемой оборудование по обеспечению защиты информации, в том числе периферийное и связное оборудование, программы испытаний технических средств, правила оформления технической документации;
- правила эксплуатации ТСЗИ и средств ВТ, исследовательских установок, измерительных приборов или технологического оборудования по ЗИ, имеющихся в подразделении, а также их обслуживание;
- вопросы обеспечения безопасности жизнедеятельности и экологии.

Освоить:

- методы анализа технического уровня обеспечения ИБ организации, аппаратного и программного обеспечения средств ЗИ для определения их соответствия действующим техническим условиям и стандартам;
- методики применения ТСЗИ, измерительной техники для контроля и изучения эффективности использования ТСЗИ и методики эксплуатации ТСЗИ;
- отдельные пакеты программных средств компьютерного обеспечения ЗИ объектов профессиональной деятельности;
- порядок пользования периодическими, реферативными и справочно-информационными изданиями по профилю направления подготовки.

Цели практики.

Целью практики является закрепление знаний и умений, полученных в процессе теоретического обучения, овладение методикой обеспечения информационной безопасности предприятия (организации), проектирования, внедрения и эксплуатации отдельных задач и подсистем комплексной системы защиты информации предприятия (организации). В процессе практики проводится изучение автоматизированных средств и систем, реализующих технологии защиты информации, обучаемый приобретает навыки исследования и проектирования подсистем обеспечения безопасности информации предприятия (организации).

Целями производственной практики являются:

- приобретение практических навыков работы в качестве специалиста (менеджера) ИБ предприятия (организации);
- приобретение навыков обслуживания средств ЗИ в ЭВМ, сетях ЭВМ и автоматизированных информационных системах;
- приобретение практического опыта разработки компонентов КСЗИ предприятия (организации);
- подготовка и систематизация необходимых материалов для построения комплексной системы защиты информации на предприятии (для выполнения курсовых работ по учебному плану);
- приобретение навыка системного подхода при проектировании КСЗИ и отдельных ее подсистем;
- приобретение навыков исследовательской и аналитической работы в области информационной безопасности.

Задачи производственной практики.

В зависимости от тематики задания руководителя практики, задачами производственной практики являются:

- приобретение практических навыков работы в качестве специалиста (менеджера)

информационной безопасности предприятия (организации);

• изучение методов обеспечения безопасности информации, применяемых на предприятии (в организации);

• освоение на практике методов предпроектного обследования объектов информатизации, проведения системного анализа результатов обследования при построении модели комплексной системы защиты информации;

• приобретение практического опыта разработки компонентов комплексной системы защиты информации предприятия (организации).

• изучение технологии регистрации, сбора, передачи и обработки информации о несанкционированных действиях, ознакомление с характеристиками периферийной, терминальной и вычислительной техники и особенностями их эксплуатации в условиях функционирования аппаратно-программных компонентов подсистем комплексной системы защиты информации.

• изучение документации комплексной системы защиты информации предприятия (организации), получение знаний по оформлению технических и рабочих проектов системы защиты информации и порядку внедрения утвержденных решений.

• привитие навыка системного подхода при проектировании комплексной системы защиты информации и отдельных ее подсистем.

• приобретение навыков выбора комплекса технических средств и сопряжения их в единую систему, расчета необходимого числа технических средств, расчета разграничения доступа к ресурсам информационной системы предприятия (организации).

• ознакомление с системной классификацией и кодированием информации, принятой в информационной системе предприятия (организации).

• ознакомление с психологическими аспектами проблемы внедрения и функционирования комплексной системы защиты информации на предприятии (в организации) и в особенности в области применения технических средств (регистраторов, сканеров, дисплеев, графопостроителей, факс–модемов, видеоконтроля и специального оборудования).

• анализ характеристик информационных процессов и формирование исходных данных для проектирования комплексной системы защиты информации предприятия (организации).

• приобретение навыков обслуживания средств ЗИ в ЭВМ, сетях ЭВМ и автоматизированных информационных системах.

• знакомство с методами и средствами обеспечения безопасности информации в документообороте, управлении бизнес-процессами и процессами административного и оперативного руководства.

• подготовка и систематизация необходимых материалов для выполнения курсового проекта (работы) по изучаемым дисциплинам и сбор материалов по выполнению выпускной квалификационной работы.

В ходе производственной практики бакалавр может выполнять следующие виды работ по заданию преподавателя:

• подготовка практических и лабораторных занятий по дисциплине (например, установка и конфигурирование необходимого программного обеспечения и оборудования, проработка задач, решаемых на занятии, сбор необходимых материалов для проведения занятия);

• подготовка учебно-методических материалов (сбор информации, выполнение обзора современных технологий, помощь в написании отдельных разделов);

• разработка прикладного (части прикладного) программного обеспечения, в том числе разработка сайтов (части сайта) и т.д.

1. ОРГАНИЗАЦИЯ ПРАКТИКИ

Кафедра своевременно готовит приказ о сроках прохождения практики, в соответствии с учебным планом и годовым календарным учебным графиком, назначает ответственного из

высококвалифицированного преподавательского состава кафедры ИЗИ ВлГУ за проведение производственной практики.

Прохождение практики состоит из следующих этапов:

Первый этап (организационный, подготовительный)

На первом этапе все студенты должны:

- самостоятельно проработать программу практики (программа выдается студентам за 1 неделю до организационного собрания);
- пройти общий инструктаж на кафедре по технике безопасности;
- ознакомиться с целью, задачами и порядком прохождения практики;
- получить индивидуальное задание по выполнению практики.

Второй этап. (Подготовка теоретических материалов). Сбор, обработка и систематизация фактического и литературного материала, в т.ч. лекций, практических занятий, методических указаний и т.д.

Третий этап. Проведение практических занятий (например, разработка программных средств, информационных систем, установка и конфигурирование необходимого программного обеспечения и оборудования и т.д.). Работа в учебных лабораториях кафедры ИЗИ по плану производственной практики.

Четвертый этап Оформление отчета по производственной практике.

Пятый этап. Защита отчета на кафедре. Защита отчета (доклад студента, ответы на вопросы) является одним из элементов подготовки молодого специалиста. Оценка по производственной практике приравнивается к оценкам по теоретическому обучению и учитывается при подведении итогов общей успеваемости студентов.

Отчет по распределенной практике в течение 6 семестра и отчет по распределенной практике по окончании 6 семестра делается совместно по одному выданному (уточненному) заданию. Защита отчета проводится после прохождения производственной практике распределенной практике по окончании 6 семестра.

2. ОРГАНИЗАЦИОННЫЕ ТРЕБОВАНИЯ К СТУДЕНТАМ

2.1. В период практики на студентов распространяется правило охраны труда и правила внутреннего распорядка, действующие в ВлГУ

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

2.3. Студенты, не выполнившие программу производственной практики без уважительной причины или получившие отрицательную оценку, могут быть отчислены из ВлГУ, как имеющие академическую задолженность, в порядке, предусмотренном Уставом ВлГУ.

3. ОБЯЗАННОСТИ СТУДЕНТОВ В ПЕРИОД ПРАКТИКИ

Студент при прохождении практики обязан:

- выполнять задания, предусмотренные общей программой практики, решать вопросы, предложенные к рассмотрению в индивидуальном задании;
- подчиняться правилам внутреннего трудового распорядка, действующим в ВлГУ или на предприятии прохождения практики;
- изучить и строго соблюдать правила эксплуатации оборудования и вычислительной техники, правила Техники безопасности, Охраны труда и другие условия работы в ВлГУ или на предприятии прохождения практики;
- над составлением отчета необходимо работать равномерно в течение всего периода практики;
- подготовиться к защите и защитить отчет в указанные сроки.

4. ОБЯЗАННОСТИ РУКОВОДИТЕЛЯ ПРАКТИКИ

• проводит организационное собрание со студентами по программе практики;
• выдает индивидуальные задания;
• составляет расписание прохождения практики в лабораториях кафедры ИЗИ;
• несет ответственность за соблюдение студентами правил ОТ и ТБ;
• осуществляет контроль за сроками прохождения практики и ее защиты.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ.

В качестве обеспечения производственной практики выступают:

- учебно-методические комплексы по дисциплинам 1-3 курсов обучения;
- кафедральная документация, методические пособия, учебники, отчеты по НИР, публикации научно-технических конференций и т.д.

Ко времени окончания практики представляется отчет о практике, подписанный руководителем практики. По итогам аттестации практики выставляется зачет с оценкой.

В состав отчёта должно входить:

- индивидуальное задание на прохождение практики, утверждённое руководителем практики;
- отчет по практике (материалы с результатами работы и предложениями);
- электронные материалы по практической работе.

Отчет о практике должен содержать следующие разделы (ориентировочный объем каждого раздела – 1-3 стр.):

- данные по изучению предметной области практики;
- кафедра и ведущий преподаватель, за которым закреплена дисциплина;
- перечень работ, выполненных бакалавром в ходе практики;
- отзыв руководителя (в дневнике практики) в произвольной форме и рекомендуемая оценка (зачет).

6. ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТНОЙ ДОКУМЕНТАЦИИ:

Структура и оформление отчетов о производственной практике должны соответствовать основным требованиям стандарта ГОСТ 7.32-2001 – «Отчет о научно-исследовательской работе – Структура и правила оформления».

Структурными элементами отчета являются:

- титульный лист;
- лист аннотации;
- содержание;
- определения;
- обозначения и сокращения;
- введение;
- основная часть;
- заключение;
- список использованных источников;
- приложения.

Они включаются в отчет строго в указанном порядке. Обязательные структурные элементы выделены полужирным шрифтом. Остальные структурные элементы включают в отчет по усмотрению исполнителя с учетом настоящих требований и требований ГОСТ 7.32-2001.

При оформлении отчетов следует придерживаться следующих правил и рекомендаций.

Титульный лист должен соответствовать форме, приведенной в Приложении. На титульном листе отчет должен быть подписан автором, консультантом (если есть), научным руководителем, заведующим кафедрой.

Лист аннотации должен содержать:

- сведения об объеме отчета (суммарное количество страниц без учета приложений), количестве иллюстраций, таблиц, приложений, количестве разделов отчета, количестве использованных источников;

- перечень ключевых слов;

- реферат отчета (не более 500 печатных знаков), в котором в краткой форме, удобной для библиотечного поиска, указываются: объект исследования или разработки, цель работы, метод проведения работы, результаты, область применения, значимость работы.

Во введении обязательно должны быть обоснованы актуальность, теоретическая и практическая значимость работы, сформулирована цель работы и перечислены задачи, решаемые для достижения поставленной цели. Объем введения, как правило, не превышает 2 – 2,5 страниц.

Основная часть, как правило, состоит из 3 - 4 самостоятельных разделов, каждый из которых характеризуется логической завершенностью и при необходимости может делиться на подразделы и пункты (заголовок «Основная часть» в отчете не пишется!). Первый раздел, как правило, содержит обзор рассматриваемой предметной области со ссылками на источники информации и постановку задачи работы. Далее следует изложение аналитических, теоретических и прикладных результатов, полученных лично автором в процессе выполнения работы (алгоритмы, протоколы, спецификации, схемы, формулы, расчеты и т.п.). Заключительные разделы содержат практические аспекты работы, описание макетной, экспериментальной части (описание разработанных программных модулей, аппаратных устройств, интерфейсов, графики или таблицы с результатами экспериментов и т.п.), обсуждение возможностей применения полученных результатов в других работах. В конце каждого раздела следует сформулировать краткие выводы (1-2 абзаца) по данному разделу. Разделы основной части должны быть пронумерованы, начиная с первого (введение к отчету и заключение не нумеруются!). Наибольший раздел не должен более, чем в 2 – 3 раза, превышать наименьший.

В заключении формулируется основной результат работы и (по пунктам) выводы по результатам выполненной работы (как правило, 3 – 5 выводов (например, один по каждому разделу)), а также указываются возможные (планируемые) пути и перспективы продолжения работы. Объем заключения, как правило, не превышает 1,5 – 2 страниц.

Отчет должен быть отпечатан шрифтом Times New Roman № 14 через 1,5 интервала на одной стороне белой бумаги формата А4. Размеры полей: сверху, снизу – 20 мм, слева – 30 мм, справа – 10 мм. Листы отчета обязательно должны быть скреплены жестким соединением и пронумерованы сквозной нумерацией, начиная с титульного листа (на котором номер не ставится). Номер страницы проставляют в центре нижней части листа без точки.

Рекомендуемый объем отчета о практике (без приложений) составляет 30–40 страниц. По тексту отчета должны содержаться ссылки на источники информации. Ссылки на публикации, приведенные в списке использованных источников, допускаются только цифровые. Разрешается использовать компьютерные возможности, применяя шрифты разной гарнитуры для акцентирования внимания на определенных терминах, формулах, теоремах и т.п. Для создания преподавателям возможности более внимательно отслеживать и анализировать материалы основные страницы сайта печатаются на принтере. Копии распечатываются на листы формата А4 в одном экземпляре. К отчету прилагается диск CD-R/RW, DVD-R/RW, содержащий все электронные материалы по работе. Переплет отчета может быть произвольным и исключать рассыпание листов.

7. ЗАЩИТА ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

Защита производственной практики проводится на заседании аттестационной комиссии кафедры в течение двух недель после начала третьего семестра.

Не позднее, чем за 3 рабочих дня до назначенной даты защиты, студентом должны быть сданы ответственному на кафедре следующие документы:

1) отчет по производственной практике на бумажном носителе, оформленный в соответствии с установленными требованиями, подписанный на титульном листе автором, и руководителем;

2) копия отчета в электронном виде (файл в формате DOC или RTF, носитель CD или DVD);

3) Заполненный дневник по практике с отзывом руководителя практики от предприятия;

4) Оценочный лист сформированности компетенций (заполняется после защиты практики руководителем практики от выпускающей кафедры с учетом отзыва руководителя практики от предприятия).

При выполнении всех вышеперечисленных требований зав. кафедрой допускает студента к защите практики на комиссии кафедры, подписывая отчет о практике (на титульном листе). К защите принимаются только работы, по оформлению и структуре полностью соответствующие установленным требованиям. Студенты, не представившие в назначенный срок все перечисленные выше документы и отчет по практике без уважительных причин, к защите не допускаются.

Для защиты практики кафедра создает комиссию из числа преподавателей – сотрудников кафедры в составе председателя комиссии и членов комиссии. Защита проводится по предварительно составленному расписанию. На защите отчета по практике студент должен иметь при себе:

1) зачетную книжку;

2) иллюстративный материал для доклада (слайды в формате Power Point, предназначенные для показа через проектор, не более 12 шт.). Все слайды выполняются в форме единой презентации. При оформлении слайдов в силу технических особенностей проекторов необходимо обращать внимание на яркость и четкость текста, рисунков, таблиц и т.д. Если мелкие детали изображения имеют первостепенное значение, фрагмент изображения следует выносить на отдельный слайд. Основной текст слайдов должен быть выполнен шрифтом размером не менее 20 или, при полужирном начертании, 18 (надписи на рисунках, в таблицах, схемах – 16 и 14 соответственно). Слайды презентации должны быть пронумерованы. Номер слайда проставляется в правом нижнем углу или по центру нижней части слайда шрифтом размером не менее 16. Использование элементов анимации, а также вставка видеофрагментов и воспроизведения звукового сопровождения презентации не разрешаются.

Защита каждой работы состоит из доклада автора работы (5 – 7 мин.) и ответов на вопросы членов комиссии. В докладе должны быть отражены:

- тема и постановка задачи практики;
- методы, пути, средства достижения поставленной в работе цели;
- полученные результаты, оценка их значимости.

Каждый член комиссии оценивает работы по четырехбальной шкале: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценка работы слагается из следующих факторов: соответствия профилю специальности, качества представленного отчета, качества доклада, конкретности, лаконичности и полноты ответов на вопросы, качества иллюстративного материала. Итоговая оценка выставляется после совещания членов комиссии с учетом оценки, рекомендованной научным руководителем. Оценки объявляются председателем комиссии по окончании работы комиссии и заносятся в зачетную книжку и в ведомость, сдаваемую в деканат.

Студенты, не защитившие отчет по производственной практике в установленный срок без уважительной причины или получившие по результатам защиты оценку «неудовлетворительно», отчисляются из университета как имеющие академическую задолженность в порядке, предусмотренном уставом ВлГУ.

Отчеты по производственной практике хранятся в архиве кафедры не менее срока обучения обучаемого.

8. ПЕРЕЧЕНЬ ПРОИЗВОДСТВЕННОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Информационно – библиотечное обеспечение – представлено в рабочих программах учебных курсов в разрезе каждой дисциплины бакалаврской программы, а также в карте обеспеченности литературой учебной дисциплины. Конкретный список рекомендованной литературы определяется руководителем практики индивидуально для каждого обучаемого в зависимости от индивидуального задания практики.

а) Основная литература:

- Тельный, А.В. Технические средства охраны : практикум для вузов / А. В. Тельный ; Владимирский государственный университет (ВлГУ) ; под ред. М. Ю. Монахова — Владимир:2012 —139с. ISBN 978-5-9984-00300-2
- Тельный, А.В.. Инженерно-техническая защита информации. Системы охранного телевидения : учебное пособие / А. В. Тельный ; Владимирский государственный университет (ВлГУ) ; под ред. М. Ю. Монахова .— Владимир 2013 .— 143 с.
- Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. ISBN 978-5-369-01378-6 Режим доступа: http://znanium.com/
- Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. ISBN 978-5-369-01378-6, Режим доступа: http://znanium.com/
- Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html. 474 с.
- Региональная и национальная безопасность: Учебное пособие / А.Б. Логунов. - 3-е изд., перераб. и доп. - М.: Вузовский учебник: НИЦ ИНФРА-М, 2014. - 457 с.: ISBN 978-5-9558-0310-4, Режим доступа: http://znanium.com/
- Кнауб, Л. В. Теоретико-численные методы в криптографии: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2012. - 160 с. Режим доступа: http://znanium.com/
- Каратунова, Н. Г. Защита информации. Курс лекций : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: http://www.znanium.comРежим доступа: http://znanium.com/
- Мишин Д.В. Анализ защищенности распределенных информационных систем. Идентификация ресурсов корпоративной сети передачи данных : практикум для вузов по направлению "Информационная безопасность" / Д. В. Мишин, Ю. М. Монахов ; Владимирский государственный университет (ВлГУ) .— Владимир : 2012 .— 94 с. ISBN 978-5-9984-0295-1.
- "Вычислительные системы, сети и телекоммуникации: учебник / А.П. Пятибратов, Л.П. Гудыно, А.А. Кириченко; под ред. А.П. Пятибратова. - 4-е изд., перераб. и доп. - М. : Финансы и статистика, 2014." - http://www.studentlibrary.ru/book/ISBN9785279032853.html 736 с.
- Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ISBN 978-5-8199-0331-5, Режим доступа: http://znanium.com/

б) Дополнительная литература:

- Башлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2, Режим доступа: http://znanium.com/
- Соколов, А.И. Технические средства защиты информации : технические каналы утечки информации : учебное пособие / А. И. Соколов, М. Ю. Монахов ; ВлГУ .— Владимир:, 2007 .— 71 с.

• Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. ISBN 978-5-369-01450-9. Режим доступа: http://znanium.com/
• Бугаков, В.П. Технические средства охраны : системы контроля и управления доступом : учебное пособие / В. П. Бугаков, А. В. Тельный ; Владимирский государственный университет (ВлГУ) .— Владимир : 2007 .— 147 с. :
• Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.: Режим доступа: http://znanium.com/
• Файман, О.И. Правовое обеспечение информационной безопасности : учебное пособие / О. И. Файман, В. А. Граник, М. Ю. Монахов ; Владимирский государственный университет (ВлГУ) .— Владимир : 2010 .— 86 с. ISBN 978-5-9984-0020-9
• Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: http://www.iprbookshop.ru/33857
• Кнауб, Л. В. Теоретико-численные методы в криптографии : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7.Режим доступа: http://znanium.com/
• Практическая криптография: алгоритмы и их программирование / Аграновский А.В., Хади Р.А. - М. : СОЛОН-ПРЕСС, 2009. - http://www.studentlibrary.ru/book/ISBN5980030026.html 256 с. ISBN 5-98003-002-6.
• Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев - М. : СОЛОН-ПРЕСС, 2009. http://www.studentlibrary.ru/book/ISBN5980030115.html 272 с.
• Воронин А.А. Вычислительные сети : учебное пособие / А. А. Воронин ; Владимирский государственный университет (ВлГУ) .— Владимир : 2011 .— 87 с. ISBN 978-5-9984-0179-A
• Основы информационных и телекоммуникационных технологий. Сетевые информационные технологии : учеб. пособие / В.Б. Попов. - М. : Финансы и статистика, 2015. - http://www.studentlibrary.ru/book/ISBN5279030139.html 224 с.
• Введение в сетевые технологии: Элементы применения и администрирования сетей: учеб. пособие / С.В. Никифоров.- 2-е изд. - М. : Финансы и статистика, 2007. - http://www.studentlibrary.ru/book/ISBN9785279032808.html 224 с.

в) Периодические издания

1. Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
2. Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.
3. Ежемесячный теоретический и прикладной научно-технический журнал «Информационные технологии». Режим доступа http://novtex.ru/IT/.

г) Программное обеспечение и Интернет-ресурсы:

1. Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
2. ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

Методические рекомендации по составлению отчета по производственной практике по типовому заданию, связанному с анализом средств обеспечения информационной безопасности на предприятии (в организации)

I. ОПИСАНИЕ ЗАЩИЩАЕМОГО ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Необходимо привести общие сведения об организации – месте прохождения практики, структурные подразделения, организационная структура. Месторасположения и т.д., обосновать актуальность проблемы защиты информации на предприятии.

II. ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

Отметить наличие на предприятии организационно-правовой документации по обеспечению информационной безопасности (Положение о коммерческой тайне на предприятии, Концепция обеспечения информационной безопасности, Политика обеспечения информационной безопасности, другие руководящие документы, положения и инструкции).
Наличие (отсутствие) специального подразделения по ЗИ, его структура, функции, должностные обязанности сотрудников
Привести (по возможности) утвержденный Перечень сведений (или ссылку на него), которые в рамках данного предприятия имеют конфиденциальный характер (составляют служебную или коммерческую тайну), а также названия документов и электронных информационных ресурсов их содержащих.
Если на предприятии Перечня нет, то привести возможный вариант сведений конфиденциального характера для данного предприятия (перечень сведений, составляющих коммерческую тайну и перечень сведений - персональных данных).

III. ОЦЕНКА УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

А. ОЦЕНКА СОСТОЯНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ УКРЕПЛЕННОСТИ ОБЪЕКТА

В данном разделе необходимо обследовать объект и его территорию (при необходимости), ***составить акт обследования*** состояния инженерно-технической укрепленности объекта и согласно РД.36.003-2002г. По категории объекта определить в каждом помещении соответствуют ли элементы технической конструкции здания (полы, стены, потолки, окна, запорные устройства) требованиям приложений РД.36.003-2002 г.

Б. СИСТЕМА ОХРАННО-ТРЕВОЖНОЙ СИГНАЛИЗАЦИИ (ОТС)

В данном разделе должны содержаться следующие краткие сведения об оснащении ОТС одного из блоков защиты (выделенная территория, здание, этаж, группа помещений):
1. Привести информацию о структуре защищаемого объекта, назначении помещений.
2. Привести перечень помещений, оборудованных ОТС.
3. Отметить наличие (или отсутствие) физической охраны объекта и место расположения поста физической охраны время несения службы.
4. Отметить наличие (или отсутствие) АРМ ОТС, возможности его комплексирования в интегрированные системы безопасности с подсистемами СОТ, СКУД, АУПС и АСПТ.
5. Привести информацию об используемых на объекте ПКП и извещателей.
Необходимо оценить правильность проведенных монтажных работ и рациональность размещения охранных извещателей согласно требований РД 78.36.003-2002г. и РД 78-145-93г.

6. Описать используемую на объекте тактику охраны и рубежность распределения шлейфов сигнализации.
7. Привести информацию о количестве и распределении ПЦН выходов от ПКП (при наличии договора на централизованную охрану).
8. Привести сведения об организации обслуживания ТСО.
Необходимо оценить структуру распределения шлейфов сигнализации (радиальная, двухпроводная линия и др.) и работоспособность средств ОТС.
Привести структурную схему ОТС и схемы распределения шлейфов сигнализации на поэтажных планах помещений.

В. СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ОБЪЕКТ (СКУД)
В данном разделе должны содержаться следующие краткие сведения об оснащении СКУД одного из блоков защиты (выделенная территория, здание, этаж, группа помещений):
1. Схема расположения защищаемых помещений или зон, размещения проходных, помещений для расположения АРМ управления.
2. Наличие физической охраны и их функции по управлению доступом.
3. Наименование объектов, оснащенных СКУД (количество точек прохода) - административные, производственные, складские, бытовые помещения, производственные площадки или внутренние территории с КПП. Тип прохода по каждой точке прохода (последовательность прохода, двухсторонний или нет, шлюз и др.).
4. Структура СКУД (сетевая, автономная), наличие АРМ, его функции и используемое программное обеспечение.
5. Элементы технической укрепленности СКУД (тамбуры, ограждения, турникеты, калитки).
Необходимо оценить рациональность выбора установленных исполнительных устройств и режима их работы.
6. Предполагаемое максимальное количество сотрудников, посетителей, единиц транспорта.
7. Пропускная способность аппаратуры СКУД и ее соответствие людским потокам.
8. Временные расписания проходов (при их наличии).
9. Тип идентификаторов пользователей (пропуска, магнитные карты, биометрия, дистанционные или контактные).
10. Краткое описание технологии работы.
11. Возможность дальнейшего расширения системы. Добавление новых точек контроля и новых АРМ.
12. Краткое описание функциональных возможностей СКУД. Обычно система должна обеспечивать:
- регистрацию и протоколирование тревожных и текущих событий;
- приоритетное отображение тревожных событий;
- управление работой преграждающими устройствами в точках доступа по командам оператора;
- задание временных режимов действия идентификаторов в точках доступа «окна времени» и уровней доступа;
- защиту технических и программных средств от НСД к элементам управления;
- автоматический контроль исправности средств, входящих в систему, и линий передачи информации;
- возможность автономной работы контроллеров системы с сохранением контроллерами основных функций при отказе связи с пунктом централизованного управления;
- установку режима свободного доступа с пункта управления при аварийных ситуациях и чрезвычайных происшествиях;
- блокировку прохода по точкам доступа командой с пункта управления.
13. Особенности технических, эксплуатационных характеристик и дизайна применяемого оборудования, наличие сертификата соответствия РФ на все применяемое оборудование.

Особенности исполнительных механизмов: типы замков, турникетов, шлюзовых кабин, замочно-переговорных устройств.

14. Особенности установки системы:

- размещение контроллеров (по месту и способу установки, подведение к ним информационных шлейфов и шин питания);
- прокладка кабельных трасс, типа кабеля, исполнения кабельных трасс или коробов (гофрошлангов, труб).
- места подключения контроллеров, блоков управления исполнительными устройствами к распределительными щитам ~220В, а также места вертикальной прокладки кабелей между этажами.

15. Оснащенность бюро пропусков комплексом для оперативного изготовления идентификационных удостоверений с фотографиями пользователей, другим специальным оборудованием.

16. Привести сведения об организации обслуживания СКУД.

Необходимо оценить количество и расположение АРМов для управления СКУД (АРМ-администраторов безопасности, АРМ-службы охраны, АРМ-бюро пропусков, АРМ службы персонала, другие АРМ). Взаимодействие АРМ СКУД с АРМ ОТС, АУПС (интеграция). Наличие сети передачи данных, связывающей объекты (АРМы системы управления доступом должны располагаться в пределах ЛВС). Защищенность АРМов СКУД от НСД.

Составляется структурная схема СКУД и схемы распределения кабельных линий на поэтажных планах помещений.

Г. СИСТЕМА ОХРАННОГО ТЕЛЕВИДЕНИЯ (СОТ)

В разделе должны содержаться следующие краткие сведения об оснащении СОТ одного из блоков защиты объекта (выделенная территория, здание, этаж, группа помещений):

1. Названия и назначения блоков внутри объекта информатизации (выделенная территория, здание, этаж, группа помещения), в которых функционирует СОТ (административные, производственные, складские, бытовые помещения, производственные площадки, смежные или внутренние территории различного назначения).
2. Количество отдельных зон, участков, объектов, оснащаемых системой (перечень защищаемых зон, территорий, отдельных зданий, выделенных участков).

Указать на схеме расположение защищаемых помещений или зон, размещения постов наблюдения. Описать по каждой зоне контроля уровень освещенности и условия видимости, климатические условия.

3. Цели наблюдения в дневном и ночном режиме (по приоритету) (Например, днем - идентификация личности, определение номера въезжающего автомобиля, ночью - обнаружение автомобиля, человека, и т. д. (с предоставлением планов зон контроля, и прилегающей территории)).
4. Решаемые системой задачи.

Например:

- контроль НСД сотрудников или нарушителей на территорию (или с территории) объекта через проходные и КПП;
- контроль НСД сотрудников или нарушителей на территорию (или с территории) объекта через ограждения или запретные зоны;
- защита людей и материальных ценностей от преступных посягательств в контролируемой зоне охраняемого объекта;
- контроль за ситуационным положением в выделенном помещении или на территории, прилегающей к объекту;
- идентификация личности посетителя или сотрудника объекта при прохождении КПП на основании данных видеотеки;
- идентификация государственного номера автомашины при проезде КПП объекта на основании баз данных службы охраны или бюро пропусков;

- контроль за действиями сотрудников определенных служб на объекте в ходе технологического процесса или исполнения ими своих служебных обязанностей;
- автоматическая фиксация и хранение в течение определенного времени записи противоправных или иных событий по тревожному извещению с защищаемого объекта;
- автоматическая фиксация и хранение в течение определенного времени (указать размер архива) всех событий с охраняемого объекта или территории.

5. Посты наблюдения и управления комплексом:
- количество независимых постов наблюдения (с указанием мест их размещения на планах);
- возможность видеорегистрации на видеорегистраторы (непрерывно, по усмотрению оператора, по сигналу охранных датчиков);
- возможность одновременного просмотра на одном мониторе всех видеокамер комплекса (всегда или только в режиме непосредственного наблюдения за объектом);
- возможность выполнять охранные функции (детекторы движения);
- возможность моментальной распечатки интересующих кадров на видеопринтере;
- возможность согласованной работы комплекса с персональным компьютером (компьютерами). В этом случае указать количество и расположение АРМов видеонаблюдения, структуру компьютерной сети на объекте.

6. Описание СОТ

Общие сведения:
- вид системы (цветная, черно-белая, комбинированная);
- срок хранения видеозаписей в архиве (обычно, одна неделя);
- возможность фиксации аудиоинформации с охраняемых объектов;
- наличие и расположение щитов электропитания вблизи мест установки оборудования и на постах наблюдения;
- наличие резервного или дублирующего питания;
- возможность дальнейшего расширения путем добавления новых телекамер и постов наблюдения (охраны);
- описание общей тактики отображения и записи информации, структуры и приоритетности защищаемых зон, порядка и уровня совмещения с взаимодействующими системами.

Технические характеристики системы:
- разрешение видеокамер, видеорегистратора;
- вид ПЗС, фокусное расстояние и параметры вариообъектовов, тип управления диафрагмой и др.

Технические характеристики устройств управления и коммутации видеосигналов:
- разрешение;
- вид входного сигнала извещения о тревоге;
- максимальные коммутируемые напряжения и ток.

Технические характеристики видеомониторов:
- разрешение;
- максимальная яркость изображения;
- геометрические и нелинейные искажения изображения.

7. Возможности системы по обеспечению нормальной устойчивости от прогнозируемых НСД и/или возможность размещения в помещениях, местах (сейфах, боксах и др.), защищенных от разрушающих механических НСД (по ГОСТ Р 50862), НСД к программному обеспечению (по ГОСТ Р 51241).

8. Возможности системы обеспечивать разграничение прав пользователей/операторов.

9. Другие технические и эксплуатационные характеристики и дизайн применяемого оборудования (наличие сертификата соответствия РФ на все применяемое оборудование; особенности видеокамер, квадраторов, мультиплексоров и другого видеооборудования по цвету, внешнему виду видеокамер и другого оборудования; особенности размещения видеокамер по месту и способу установки видеокамер; особенности прокладки кабельных трасс: типу кабеля, исполнения кабельных трасс или коробов (гофрошлангов, труб)).

10. Привести сведения об организации обслуживания СОТ.

Данный раздел должен обязательно содержать:
- структурную (функциональную) схему размещения видеокамер на объекте, с указанием места ее установки и зоны обзора, оборудования системы и постов охраны СОТ;
- спецификацию (технические характеристики) поставляемого оборудования и программного обеспечения.

Д. КОРПОРАТИВНАЯ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ

Сведения об объекте защиты

1. Объекты, подлежащие оснащению комплексом защиты корпоративной сети (наименование, характеристика деятельности).
2. Решаемые комплексом защиты проблемы (как минимум контроль НСД). Общие данные о функционировании информационной системы.
3. Порядок назначения прав по доступу к критичным ресурсам.
4. Регламент резервирования и восстановления критичной информации.
5. Наличие ответственного администратора сети (безопасности сети).
6. Расположение критичной информации.
7. Информационные потоки критичной информации, относительно рабочих станций, серверов, сегментов.
8. Наличие систем электронного документооборота.
9. Наличие критичных для предприятия процессов электронной обработки и передачи данных.
10. Возможность круглосуточной работы.

Информация о топологии сети, сетевых соединениях и узлах

11. Карта сети:
- количество и тип серверов (платформы, операционные системы, сервисы),
- приложения,
- количество и тип рабочих станций (платформы, ОС, приложения, решаемые задачи),
- используемые сетевые протоколы.

12. Указать на схеме сегменты и способы их соединения (маршрутизаторы, хабы, мосты и прочее).
13. Указать вариант организации выхода в Internet:
- подключение выделенного компьютера (способ подключения, авторизации и пр.);
- подключение сети (способ подключения, использование прокси-служб и прочее);
- необходимость контроля трафика и разграничения доступа пользователей;
- наличие внутри предприятия собственного WEB, FTP серверов.

Использование встроенных (приобретенных) средств мониторинга, безопасности и архивации

14. Защита ПК от НСД (аудит, разграничение доступа), защита и разграничение доступа к ПК при работе на них нескольких пользователей.
15. Межсетевые экраны - защита от внешних/внутренних атак.
16. Системы авторизации.
17. Антивирусная защита.
18. Средства архивирования, режим их работы.
19. Системы протоколирования действий пользователей.
20. Криптографическая защита.
21. Средства системного аудита.
22. Системы мониторинга сети.
23. Защита вычислительной техники от взлома, краж.
24. Анализаторы протоколов.

25. Сканеры - сканирование ресурсов сети на возможные уязвимости и выдача рекомендаций для их устранения.
26. Разделение критичных сегментов сети.
27. Системы мониторинга безопасности - проверка правильности настройки корпоративных серверов, мониторинг безопасности корпоративной сети в реальном времени.

Особенности функционирования комплекса
28. Возможности дальнейшего расширения путем добавления (каких систем, устройств).
29. Необходимость и условия совместимости с существующими (или проектируемыми), системами (элементами) автоматизации учета, технологического процесса на объектах.
30. Необходимость и условия совместимости с существующими (или проектируемыми) системами (элементами) систем безопасности корпоративной сети объекта.
31. Наличие сертификата соответствия РФ на все применяемое оборудование: классы защищенности АС, СВТ (операционной системы), межсетевых экранов, антивирусных средств, уровень анализа программного обеспечения на недекларированные возможности.
Данный раздел должен содержать:
- структурную (функциональная) схема сети с указанием элементов комплекса защиты;
- спецификации (технические характеристики) оборудования и программного обеспечения комплекса.

Е. СИСТЕМА ПРОТИВОДЕЙСТВИЯ ЭКОНОМИЧЕСКОМУ ШПИОНАЖУ (СПЭШ) В ВЫДЕЛЕННОМ ПОМЕЩЕНИИ

Общие сведения о защищаемом объекте.
1. Список и местоположение (здание, этаж) помещений, подлежащих оснащению СПЭШ. К таким помещениям могут относиться:
- выделенные помещения, предназначенные для ведения переговоров и совещаний;
- кабинеты руководства и другие помещения, в которых проводятся конфиденциальные переговоры и совещания;
- прочие технологические помещения, в которых циркулирует информация, предназначенная для служебного пользования.
2. Каналы связи, подлежащие защите:
- выделенные каналы, предназначенные для передачи секретной информации;
- каналы, по которым передается конфиденциальная информация;
- каналы, по которым передается информация для служебного пользования.
3. Степень конфиденциальности (секретности) информации, циркулирующей и размещенной на объекте информатизации.
4. Площадь защищаемых помещений объекта (кв.м).
5. Тип наружных стен, перегородок и межэтажных перекрытий (потолок, пол), (капитальные: бетонные толщиной более 200 мм или кирпичные толщиной более 500 мм).
6. Входы в помещения. Тамбуры (двойные двери), расстояние между дверями. Двери: тип конструкции, наличие уплотнения, запорные устройства.
7. Окна: количество проемов, тип остекления, наличие и тип защитных пленок.
8. Тип и высота потолков (подвесные с зазором, подшивные, оштукатуренные, иные).
9. Описание смежных помещений: примыкающих к стенам объекта, над и под объектом. Назначение помещений или характер проводимых в них работ.
10. Организация контроля и управления доступом на объект в целом и в выделенные помещения.
11. Имеющиеся на объекте средства связи: пользователь средства связи, стандарт или принцип действия, наименование или тип аппаратуры, количество каналов. В том числе линии телефонной связи: количество входящих линий городской и внутренней телефонной сети.

12. Система электропитания и освещения: источники питания, расположение трансформаторной развязки.
13. Система заземления: наличие, структура контура заземления, сопротивление.
14. Системы сигнализации (тип).
15. Прочие проводные линии: радиотрансляция (местная, городская), электрочасофикация (марка).
16. Наличие специальных технических средств защиты информации.
17. Схема помещения и расположения в нем мебели и других предметов интерьера (с указанием основных размеров или масштаба).

Описание обстановки вокруг объекта защиты

18. Описание соседних строений: назначение (характер проводимых там работ), этажность, расстояние до защищаемого помещения.
19. Наличие и удаленность автостоянки.
20. Архитектурные или технические особенности защищаемых помещений, особенности расположения помещений внутри здания.
21. Система вентиляции на объекте (тип).
22. Система отопления.
23. Имеющаяся оргтехника.
24. Имеющаяся бытовая техника: телевидение (марка телевизора), кабельное телевидение, антенна внешняя (комнатная).

Анализ информационных угроз

25. Определение видов информационных угроз в помещениях и технических каналах.
<u>С проникновением на объект:</u>
- внедрение специальных устройств с целью перехвата информационных сигналов, их преобразования и передачи за пределы зоны безопасности объекта по различным каналам;
- несанкционированная запись информационных сигналов с использованием средств регистрации информации.
<u>Без проникновения на объект:</u>
- прослушивание каналов связи;
- преднамеренный разрыв каналов связи;
- перехват остаточных информационных сигналов и электромагнитных излучений, распространяющихся за пределы зоны безопасности.
26. Определение видов перехватываемой информации в основных каналах утечки информации:
- акустический канал - речевые и прочие акустические сигналы;
- виброакустический канал - речевые и прочие акустические сигналы;
- утечка по проводному каналу - речевые и прочие акустические сигналы, факсимильная, телеграфная, телетайпная информация, информация, обрабатываемая на ЭВМ, или транслируемая по модемным каналам;
- электромагнитные поля - информация передаваемая по радиотелефону и радиосвязи, информация, передаваемая по радиомодему;
- ПЭМИН - информация, обрабатываемая на ЭВМ, ПЭМИН прочего офисного оборудования, промодулированный полезным акустическим сигналом;
- оптический - скрытая фото, кино и видеосъемка, видеонаблюдение из вне зоны охраны.
27. Оценка оперативно-тактических возможностей нарушителя. Формирование модели нарушителя, его возможностей по:
- перехвату информации в непосредственной близости от территории объекта,
- легальному проникновению на территорию объекта, например, иметь статус сотрудника родственного предприятия или клиента,

- временному использованию или стационарной установке технических средств промышленного шпионажа,
- получению априорных данных, которые могут облегчить планирование и проведение операций по перехвату информации.

К таким данным относятся, например:
- тематика перехватываемой информации,
- сведения о перечне решаемых вопросов,
- технические средства хранения, обработки и передачи информации, общие параметры сигналов, несущих полезную информацию,
- расположение помещений,
- организация и техническая оснащенность службы безопасности,
- распорядок работы объекта,
- психологическая обстановка в коллективе.

28. Оценка технического оснащения нарушителя по следующим группам технических средств перехвата и регистрации информации:
- радиомикрофоны (перехват акустической информации);
- телефонные радиопередатчики (перехват телефонной информации);
- системы кабельных микрофонов (перехват акустической информации;
- системы с передачей информации по сетям электропитания и телефонным линиям (перехват акустической информации).
- направленные микрофоны (перехват акустической информации;
- комплексы для перехвата информации с монитора ЭВМ в реальном времени;
- стетоскопы (перехват акустической информации);
- аппаратура для перехвата остаточных информативных сигналов в линиях питания и заземления;
- аппаратура для перехвата радиоэфирной информации и ПЭМИН офисного оборудования;
- звукозаписывающая аппаратура (перехват акустической информации).

29. Оценка технических возможностей потенциального нарушителя с учетом его финансового положения и целесообразности вложения средств в конкретную операцию по перехвату информации. Обычно количество вложенных средств пропорционально стоимости интересующей нарушителя информации.

Функции специального оборудования.

30. Защита от утечек информации по акустическому каналу, за счет: ПЭМИН средств ВТ и звукоусилительной аппаратуры, по цепям питания и заземления, по каналу визуального наблюдения, виброакустическому каналу.

31. Защита от утечек по проводному каналу - речевые и прочие акустические сигналы, факсимильная, телеграфная, телетайпная информация, информация, обрабатываемая на ЭВМ, или транслируемая по модемным каналам.

32. Защита от утечек через электромагнитные поля - информация передаваемая по радиотелефону и радиосвязи, информация, передаваемая по радиомодему.

33. Защита от утечек через ПЭМИН - информация, обрабатываемая на ЭВМ, ПЭМИН прочего офисного оборудования, промодулированный полезным акустическим сигналом;

34. Защита от утечек через оптический канал - скрытая фото, кино и видеосъемка, видеонаблюдение из вне зоны охраны.

Технология работы СПЭШ

35. Система защиты информации (СЗИ) должна обеспечивать оперативное и незаметное для окружающих выявление активных радиомикрофонов, занесенных в помещение, имеющих традиционные каналы передачи информации.

36. Аппаратура СЗИ по акустическому и вибро-акустичекому каналу должна включаться в работу по команде оператора.

37. Включение аппаратуры защиты информации от съема с использованием записывающих устройств должно управляться оператором.

38. СЗИ должна обеспечивать противодействие перхвату информации, передаваемой по телефонной линии (на участке до АТС).

Функциональные возможностям СПЭШ

39. Система должна обеспечивать защиту информации от утечек:

- по акустическому каналу с использованием различной звукозаписывающей аппаратуры, внесенной на объект;
- по акустическому каналу в виде мембранного переноса речевых сигналов через перегородки за счет малой массы и слабого затухания сигналов;
- по акустическому каналу за счет слабой акустической изоляции (щели у стояков системы отопления, вентиляция);
- по виброакустическому каналу за счет продольных колебаний ограждающих конструкций и арматуры систем отопления;
- по проводному каналу от съема информации с телефонной линии (городская и внутренняя телефонная сеть, факсимильная связь, переговорные устройства, системы конференц-связи и оповещения, системы охранной и пожарной сигнализации, сети электропитания и заземления);
- по каналу электромагнитных полей основного спектра сигнала за счет использования различных радиомикрофонов, телефонных радиопередатчиков;
- по оптическому каналу за счет визуального наблюдения за объектом с использованием технических средств;
- по каналу ПЭМИН за счет модуляции полезным сигналом электромагнитных полей, образующихся при работе бытовой техники;
- по каналу ПЭМИН при обработке информации на ПЭВМ за счет паразитных излучений компьютера.

Стационарные средства защиты информации

40. Определение стационарных средств защиты информации в выделенном помещении для проведения переговоров и совещаний. Обычно используются следующие виды технических средств:

- система, блокирующая передачу информации по сети питания,
- средство блокировки виброканала,
- обнаружитель работающих диктофонов,
- подавитель радиомикрофонов и диктофонов,
- генераторы акустического шума,
- стационарный детектор электромагнитного поля.

41. Определение стационарных средств защиты информации в кабинетах руководства и помещениях, в которых проводятся переговоры и совещания. Обычно используются следующие виды технических средств:

- комплексный генератор шума,
- система вибродатчиков,
- обнаружитель работающих диктофонов,
- подавитель радиомикрофонов и диктофонов,
- генераторы акустического шума,
- стационарный индикатор электромагнитного поля,
- фильтры для проводных линий.

42. Определение стационарных средств защиты информации в прочих технологических помещениях, в которых циркулирует информация, предназначенная для служебного пользования. Обычно используются следующие виды технических средств:

- фильтры для проводных линий,
- при наличии в помещениях ПЭВМ должны быть установлены генераторы радиоэлектронного шума (в варианте защиты рабочего места).

43. Определение стационарных средств защиты информации в выделенных каналах связи для передачи:

- секретной информации,
- конфиденциальной информации,
- информации для служебного пользования.

Данный раздел должен содержать:

- план выделенного помещения;

- структурную (функциональную) схему размещения оборудования СПЭШ,

- спецификацию (технические характеристики) применяемого оборудования и программного обеспечения.

В конце каждого раздела А-Е в должны быть представлены:

- краткий перечень выявленных недостатков (несоответствие требованиям нормативных документов) обеспечения безопасности по тематике раздела;

- краткие предложения по обеспечению должного уровня безопасности объекта по тематике раздела. Недостатки и предложения должны быть как технического, так и организационного характера.

Приложение №1

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Кафедра информатики и защиты информации
ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И
РАДИОЭЛЕКТРОНИКИ

ОТЧЕТ
по производственной практике

«*Тема работы*»

Исполнитель:

студент(ка) гр. ___ _____ Фамилия И.О.
(подпись, дата)

Научный руководитель:

_____ Фамилия И.О.
(подпись, дата)

Заведующий кафедрой:

_____ Фамилия И.О.
(подпись, дата)

Владимир 20__

Приложение 2

УТВЕРЖДАЮ
Заведующий кафедрой ИЗИ
_____М.Ю. Монахов
«____»_____20__г.

ЗАДАНИЕ

на производственную практику студента _____
(фамилия, имя, отчество)

___курса, специальности_____ группы _____
Предприятие_ ВлГУ

Последовательность прохождение практики:

_____

_____

_____

_____

_____

За время прохождения практики необходимо:

_____

_____

_____

_____

_____

_____

Задание по стандартизации отчет должен быть выполнен в соответствии с ГОС Т 7.32-2001. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно - исследовательской работе, структура и правила оформления.

Отчет по практике составить до _____.
Задание выдал: _____
(подпись и ФИО преподавателя, дата)

Задание получил: _____
(подпись и ФИО студента, дата)
Примечание: задание должно быть приложено к отчету по практике (вторым листом после титульного листа)

Приложение 3

ОЦЕНОЧНЫЙ ЛИСТ

результатов прохождения производственной практики по направлению подготовки 10.03.01 «Информационная безопасность»

Студент_____ **Институт** **ИИТР**

(Фамилия, И., О.)

Группа _____ **Курс**_____ **Кафедра** ИЗИ

Оценочный материал

			Оценка			
	ОБЩАЯ ОЦЕНКА *(отмечается руководителем практики от профильной организации знаком * в соответствующих позициях графы «оценка»)*		**5**	**4**	**3**	**2**
1	Уровень подготовленности студента к прохождению практики					
2	Умение правильно определять и эффективно решать основные задачи					
3	Степень самостоятельности при выполнении задания по практике					
4	Инициативность					
5	Оценка трудовой дисциплины					
6	Оценка уровня выполнения индивидуальных заданий					
	№ по ФГОС	**СФОРМИРОВАННЫЕ В РЕЗУЛЬТАТЕ ПРАКТИКИ КОМПЕТЕНЦИИ** *(отмечаются руководителем практики от университета знаком * в соответствующих позициях графы «оценка»)*	**Оценка**			
			5	**4**	**3**	**2**
Обще-культурные	*ОК-8*	способность к самоорганизации и самообразованию				
Профессиональные	*ОПК-1*	способность анализировать физические явления и процессы для решения профессиональных задач				
	ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач				
	ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации				
	ОПК-5	способность использовать нормативные правовые акты в профессиональной деятельности				
	ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты				
Профессиональные	*ПК-1*	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации				
	ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач				
	ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты				
	ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты				
	ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации				
	ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации				

	ПК-7	способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений				
	ПК-8	способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов				
	ПК-9	способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности				
	ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности				
	ПК-11	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов				
	ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации				
	ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации				
	ПК-14	способность организовывать работу малого коллектива исполнителей в профессиональной деятельности				
	ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю				
Профессионально-специализированные	*ПСК-3.1*	способность проводить совместный анализ функционального процесса объекта защиты и применяемых информационных технологий и технических средств, с целью определения возможных источников информационных угроз, их вероятных целей и тактики				
	ПСК-3.2	способность формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта и его информационных составляющих, с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объектов и локализации защищаемых элементов				
	ПСК-3.3	способность разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение				
	ПСК-3.4	способность организовать и сопровождать аттестацию объектов информатизации в соответствии с нормативными документами				
ИТОГОВАЯ ОЦЕНКА (определяется средним значением оценок по всем пунктам)						

Замечания и пожелания _____

_____

_____

Руководитель практики
от университета _____ _____

Руководитель практики
от профильной организации _____ _____
(число и подпись) (расшифровка подписи)

М.П.

Методические указания составлены в соответствии с требованиями ФГОС по направлению подготовки 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»

Методические указания разработал доцент кафедры ИЗИ к.т.н. Тельный А.В.
(ФИО, подпись)

Методические указания рассмотрены и одобрены на заседании кафедры ИЗИ

Протокол № 7 от 28.12.16 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Методические указания рассмотрены и одобрены на заседании учебно-методической направления 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»

Протокол № 4 от 28.12.16 года

Председатель комиссии д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)