Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

Перцева И.А.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

при прохождении практики

Для студентов по специальностям 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения

Ульяновск, 2019

Методические указания для самостоятельной работы при прохождении практики/ составитель: И.А.Перцева. - Ульяновск: УлГУ, 2019. Настоящие методические указания предназначены для студентов по специальностям 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения. В работе приведены рекомендованная литература по дисциплине, основные этапы прохождения практики, рекомендации по выполнению работ на каждом этапе, контрольные вопросы для самоконтроля и тесты для самостоятельной работы. Студентам очной формы обучения они будут полезны при подготовке и прохождении учебной и производственной практики, подготовке к зачёту по практике.

Рекомендованы к введению в образовательный процесс Ученым советом Факультета математики, информационных и авиационных технологий УлГУ (протокол № 2/19 от 19 марта 2019 г.).

Содержание

1. ЛИТЕРАТУРА

рекомендованная к изучению

1. Защита информации: основы теории: учебник для бакалавриата и магистратуры / Щеглов А. Ю., Щеглов К. А. – М.: Издательство Юрайт, 2019. – 309 с.https://biblio-online.ru/viewer/zaschita-informacii-osnovy-teorii-433715
2. Новиков В.К., Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]: Учебное пособие. / В.К. Новиков - М.: Горячая линия - Телеком, 2015. - 176 с. - ISBN 978-5-9912-0525-2 – Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991205252.html.
3. Некоммерческая интернет-версия СПС "КонсультантПлюс":
   - Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации". Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/
   - Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Режим доступа http://www.consultant.ru/document/cons_doc_LAW_61801/
   - Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/.
   - Положение о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования (утв. приказом Министерства образования и науки РФ от 27 ноября 2015 г. № 1383). Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_190917/ .
   - Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/
   - Постановление Правительства РФ от 3 февраля 2012 г. N 79 «О лицензировании деятельности по технической защите конфиденциальной информации».
   - Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти. Постановление Правительства РФ от 3 ноября 1994г. № 1233
   - Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины

информационной безопасности Российской Федерации") Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

- Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации") Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/

4. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.
5. Прикладная дискретная математика [Электронный ресурс]: Междунар. ежекварт.журнал. –Томск., 2017-2019.- ISSN 2311-2263.Режим доступа: http://journals.tsu.ru/pdm/&journal_page=archive&id=1823
6. Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск : УлГУ, 2016. - 1 электрон. опт. диск (CD-ROM). **URL:** http://edu.ulsu.ru/cources/750/interface/.
7. Основы информационной безопасности. Курс лекций. Часть 1 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2020 – 63 с.
8. Основы информационной безопасности. Курс лекций. Часть 2 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2020 – 103 с.
9. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М.: Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204705.html.
10. Бузов Г.А., Защита информации ограниченного доступа от утечки по техническим каналам [Электронный ресурс] / Г.А. Бузов - М.: Горячая линия - Телеком, 2015. – 586 с. - ISBN 978-5-9912-0424-8 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204248.html
11. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»; ИНФРА-М, 2014. – 416 с. ил.
12. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.: РИОР: ИНФРА-М, 2015. - 392с.
13. Инженерно-техническая защита информации: учебное пособие для студентов, обучающихся по специальностям в области

информационной безопасности / А.А. Торокин. М.: Гелиос АРВ, 2005, 960 с.
14. Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации: Учебное пособие. Изд. 4-е, перераб. и доп. – М.:ЛЕНАНД, 2016. – 416.с.
15. Рацеев С.М. Математические методы защиты информации [Электронный ресурс]: Электронное учеб. пособие. – Ульяновск: УлГУ, 2018. 1 CD-R. № гос. регистрации – 0321901084.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Практика направлена на закрепление студентами теоретических и практических знаний, полученных в процессе обучения, овладение необходимыми профессиональными навыками работы и решение практических задач, приобретение опыта работы в коллективе.

В ходе практики студент должен получить необходимое профессиональное представление и приобрести профессиональные навыки работы в отделах, службах и подразделениях, используя теоретические знания, полученные в процессе учебы и в результате работы над выполнением задания на практику.

Для успешного прохождения практики необходимо ознакомиться со структурой практики, самостоятельно изучить представленные источники литературы.

На каждом этапе осуществляется текущий контроль за процессом формирования необходимых компетенций.

2.1. РАЗДЕЛ 1. ПОДГОТОВИТЕЛЬНЫЙ ЭТАП

Подготовительный этап включает следующие мероприятия:

- проведение организационных собраний студентов, направляемых на практику для ознакомления с целями и задачами практики, этапами ее проведения, информацией о предприятиях – базах практики;
- проведение инструктажа по ТБ и должностным обязанностям студентов, направляемых на практику, с соответствующей записью в журнале по ТБ;
- определение задач на практику и плана работ. Содержание индивидуальных заданий и планируемые результаты прохождения практики отражаются в дневнике по практике (см. приложение 1).

Примерные формулировки индивидуальных заданий на практику:

1. Изучить средства защиты баз данных, ОС, антивирусные средства и др., имеющиеся на предприятии

2. Изучить имеющиеся на предприятии инструкции (руководства) по пропускному режиму, по обеспечению информационной безопасности (перечни сведений, составляющих коммерческую тайну, персональные данные и др., соглашения о неразглашении и др.)
3. Ознакомиться с имеющимися на предприятии криптографическими средствами защиты информации и документацией на них
4. Изучить должностные инструкции специалистов по ИБ предприятия.
5. Изучить имеющиеся на предприятии доступные руководящие документы, касающиеся защиты информации
6. Дать качественную и точную количественную оценку последствий реализации угроз на предприятии (или в организации)
7. Изучить разнообразные технические средства, которые препятствуют нанесению убытков предприятию
8. Изучить регламентацию производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, которая исключает или ослабляет нанесение каких-либо убытков предприятию
9. Изучить доступные методы и средства инженерной защиты объектов информатизации предприятия
10. Изучить доступные программные и аппаратные средства защиты информации от несанкционированного доступа на предприятии
11. Изучить специальные законы, другие нормативные акты, правила, процедуры и мероприятия, которые применяются на предприятии (или в организации) для защиты информации на правовой основе
12. Изучить защитные мероприятия, применяемые на предприятии, ориентированные на защиту информации от разглашения, утечки и несанкционированного доступа

2.2. РАЗДЕЛ 2. ЭКСПЕРИМЕНТАЛЬНЫЙ ЭТАП

В соответствие с полученным индивидуальным заданием студент проводит сбор, обработку, систематизацию материалов по теме исследования. Далее проводится решение задач, разработка алгоритмов и создание прикладных программ, необходимых для достижения целей.

Экспериментальный этап проходит на утвержденной базе практики в форме самостоятельной практической работы студента под руководством куратора/наставника от предприятия.

Во время проведения этапа студентам необходимо:

- соблюдать трудовую дисциплину, правила техники безопасности,

пожарной безопасности, производственной санитарии, выполнять требования внутреннего распорядка предприятия;

- ежедневно согласовывать состав и объём работ с наставником;
- информировать наставника о своих перемещениях по территории предприятия в нерабочее время с целью выполнения отдельных заданий;
- вести записи в дневниках в соответствии с индивидуальным планом;
- принимать участие в групповых или индивидуальных консультациях с руководителем практики от образовательного учреждения и предъявлять для проверки результаты выполнения заданий в соответствии с индивидуальным планом;
- с разрешения (руководителя практики от предприятия/наставника) участвовать в производственных совещаниях, планёрках и других административных мероприятиях.

Примерные тестовые для текущего контроля и самоконтроля

Какие меры позволяют структурировать средства достижения информационной безопасности, входят: a) меры обеспечения целостности; b) административные меры; c) меры обеспечения конфиденциальности
Какой угрозой является дублирование сообщений: a) доступности; b) конфиденциальности; c) целостности.
Кто является обладателем информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений? а) Работник б) Работодатель в) Пенсионный фонд г) Налоговая служба
На какие документы, из перечисленных, следует опираться при создании системы защиты ПДн на предприятии? Выбрать 2 позиции. а) № 149-ФЗ «Об информации, информационных технологиях и о защите информации» б) ПП РФ N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" в) Конституция РФ г) N 152-ФЗ «О персональных данных»
Чем технические средства расширяют и дополняют возможности человека по добыванию информации? а) Возможностью консервировать информацию на непродолжительное время б) Съемом информации с носителей, которые недоступны органам чувств человека в) Возможностью добычи информации за пределами контролируемой зоны
Какой документ, из перечисленных, не относится к сфере противодействия иностранным техническим разведкам? а) Федеральный закон от 27 декабря 2002 г. № 184 - ФЗ «О техническом регулировании» б) Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации»

в) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» г) Указ Президента Российской Федерации от 16 августа 2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»
Кто несет ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти и в организациях? а) Заместитель руководителя организации по безопасности б) Руководитель организации в) Начальник режимно-секретного подразделения
Объектом интеллектуальной собственности не является: а) Программа для ЭВМ б) Юридический документ в) Базы данных г)Секреты производства
Самыми опасными источниками внутренних угроз являются: a) некомпетентные руководители; b) обиженные сотрудники; c) любопытные администраторы.
Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности. a) просчеты при администрировании информационных систем; b) необходимость постоянной модификации информационных систем; c) сложность современных информационных систем.
Агрессивное потребление ресурсов является угрозой: a) доступности b) конфиденциальности c) целостности
Окно опасности появляется, когда: a) становится известно о средствах использования уязвимости; b) появляется возможность использовать уязвимость; c) устанавливается новое ПО
Среди ниже перечисленных отметьте две троянские программы: a) I LOVE YOU; b) Back Orifice; c) Netbus
Уголовный кодекс РФ не предусматривает наказания за: a) создание, использование и распространение вредоносных программ; b) ведение личной корреспонденции на производственной технической базе; c) нарушение правил эксплуатации информационных систем
Под определение средств защиты информации, данное в Законе «О государственной тайне», подпадают: a) средства выявления злоумышленной активности; b) средства обеспечения отказоустойчивости; c) средства контроля эффективности защиты информации
В число целей политики безопасности верхнего уровня входят: a) решение сформировать или пересмотреть комплексную программу безопасности; b) обеспечение базы для соблюдения законов и правил; c) обеспечение конфиденциальности почтовых сообщений
В число целей политики безопасности верхнего уровня входят: a) управление рисками; b) определение ответственных за информационные сервисы; c) определение мер наказания за нарушения политики безопасности

В рамках политики безопасности нижнего уровня осуществляются: a) стратегическое планирование; b) повседневное администрирование; c) отслеживание слабых мест защиты
Политика безопасности строится на основе: a) общих представлений об ИС организации; b) изучения политик родственных организаций; c) анализа рисков
Риск является функцией: a) размера возможного ущерба; b) числа пользователей информационной системы; c) уставного капитала организации
В число этапов управления рисками входят: a) идентификация активов; b) ликвидация пассивов; c) выбор объектов оценки
Первый шаг в анализе угроз — это: a) идентификация угроз; b) аутентификация угроз; c) ликвидация угроз.
Оценка рисков позволяет ответить на следующие вопросы: a) чем рискует организация, используя информационную систему? b) чем рискуют пользователи информационной системы? c) чем рискуют системные администраторы?
В число классов мер процедурного уровня входят: a) поддержание работоспособности; b) поддержание физической формы; c) физическая защита
В число принципов управления персоналом входят: a) минимизация привилегий; b) минимизация зарплаты; c) максимизация зарплаты
В число этапов процесса планирования восстановительных работ входят: a) выявление критически важных функций организации; b) определение перечня возможных аварий; c) проведение тестовых аварий
Протоколирование и аудит могут использоваться для: a) предупреждения нарушений ИБ; b) обнаружения нарушений; c) восстановления режима И Б
Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами: a) выработка и проведение в жизнь единой политики безопасности; b) унификация аппаратно-программных платформ; c) минимизация числа используемых приложений
Экранирование может использоваться для: a) предупреждения нарушений И Б; b) обнаружения нарушений; c) локализации последствий нарушений
В число основных принципов архитектурной безопасности входят: a) следование признанным стандартам; b) применение нестандартных решений, не известных злоумышленникам;

c) разнообразие защитных средств
Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами: a) использование собственных линий связи; b) обеспечение конфиденциальности и целостности при сетевых взаимодействиях; c) полный анализ сетевого трафика
В число универсальных сервисов безопасности входят: a) управление доступом; b) управление информационными системами и их компонентами; c) управление носителями
Контроль целостности может использоваться для: a) предупреждения нарушений И Б; b) обнаружения нарушений; c) локализации последствий нарушений
В число универсальных сервисов безопасности входят: a) средства построения виртуальных локальных сетей; b) экранирование; c) протоколирование и аудит
В качестве аутентификатора в сетевой среде могут использоваться: a) кардиограмма субъекта; b) номер карточки пенсионного страхования; c) результат работы генератора одноразовых паролей
Аутентификация на основе пароля, переданного по сети в зашифрованном виде, плоха, потому что не обеспечивает защиты от: a) перехвата; b) воспроизведения; c) атак на доступность
Цифровой сертификат содержит: a) открытый ключ пользователя; b) секретный ключ пользователя; c) имя пользователя
Кто является обладателем информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений? а) Работник б) Работодатель в) Пенсионный фонд г) Налоговая служба
Какой организации следует отправлять Уведомление о намерении осуществлять обработку ПДн, если организация является оператором по обработке ПДн? а) Роскомнадзор б) ФСТЭК в) Налоговая служба г) ФСБ
На кого возлагается организация сертификации средств ЗИ? Выбрать 3 позиции. а) ФСТЭК б) МВК по ЗГТ в) ФСБ г) Аттестационная комиссия д) МО РФ
Какая организация занимается координацией работ по организации сертификации? а) ФСТЭК б) МВК по ЗГТ

в) ФСБ
Какие органы, из перечисленных, уполномочены на ведение лицензионной деятельности? Отметить 2 позиции. а) ФСТЭК б) СВР РФ в) МВК г) ФСБ РФ
Организация подает документы на получение лицензии. В течение какого времени орган, уполномоченный на ведение лицензионной деятельности, принимает решение о выдаче или об отказе в выдаче лицензии? а) В течение 7 дней б) В течение 30 дней в) В течение 15 дней
В течение какого времени организация должна подать заявление о переоформлении лицензии, если изменились условия ведения лицензируемого вида деятельности? а) В течение 7 дней б) В течение 30 дней в) В течение 15 дней
Какая организация занимается лицензированием деятельности по ТЗИ конфиденциальной информации? а) ФСТЭК б) МВК в) ФСБ
Объектом интеллектуальной собственности не является: а) Программа для ЭВМ б) Юридический документ в)Базы данных г)Секреты производства
В каких правах может быть ограничено лицо, допущенное или ранее допускавшееся к ГТ? а) В праве на неприкосновенность частной жизни во время оформления допуска к ГТ б) В праве выезжать за пределы города, в котором проживает в) В праве вступать в брак
Какой федеральный орган исполнительной власти является уполномоченным в области технической защиты информации? а) Минобороны России б) ФСТЭК России в) ФСБ
С чьей санкции осуществляется взаимная передача сведений, составляющих государственную тайну, между организациями, не состоящими в отношениях подчиненности и не выполняющими совместных работ? а) Органа, уполномоченного на ведение лицензионной деятельности в области защиты государственной тайны б) Органа государственной власти, в распоряжении которого находятся эти сведения в) ФСТЭК
Основанием для освобождения руководителей организаций от государственной аттестации является: а) Наличие у руководителя допуска к государственной тайне по второй форме б) Наличие стажа работы в сфере защиты государственной тайны более 5 лет в) Наличие документа об образовании и (или) о повышении квалификации, выданного организацией, включенной в перечень, определяемый МВК по ЗГТ, если со времени ее

окончания прошло не более 5 лет
Какой документ, из перечисленных, не относится к сфере противодействия иностранным техническим разведкам? а) Федеральный закон от 27 декабря 2002 г. № 184 - ФЗ «О техническом регулировании» б) Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации» в) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» г) Указ Президента Российской Федерации от 16 августа 2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»
К основным источникам функциональных сигналов относятся: а) Излучатели акустических сигналов гидролокаторов и акустической связи б) Электропроводящие коммуникации здания, проходящие через контролируемую зону в) Средства мобильной телефонной и радиосвязи
Емкостная паразитная связь образуется в результате: а) Воздействия магнитного поля б) Воздействия электрического поля в) Воздействия активного сопротивления
Низкочастотное излучение – это: а) Электромагнитные поля, частота которых соответствует звуковому диапазону б) Электромагнитные поля, излучаемые цепями радиоэлектронных средств
Что из перечисленного относится к случайным акустоэлектричесим преобразователям? а) Металлические корпуса средств и приборов б) Монтажные провода, соединительные кабели, токопроводы печатных плат в) Ферромагнитные материалы в виде сердечников трансформаторов и дросселей
К излучающим элементам ВЧ-навязывания относятся: а) Токопроводящие механические конструкции, изменяющие свой размер и переотражающие внешнее электромагнитное поле б) Электронно-лучевые трубки средств отображения защищаемой информации в) Цепи, содержащие случайные акустоэлектрические преобразователи
Основным распределенным источником магнитного, электрического и электромагнитного полей является: а) Анизотропный излучатель б) Симметричный/несимметричный кабель в) Цепь звукоусилительной аппаратуры г) Кабель внутренней АТС
Цепи заземления в общем случае создаются для выполнения следующих функций: а) Создание электрического поля б) Модуляция тока электропитания токами радиоэлектронного средства в) Обеспечение путей для протекания возвратных (обратных) питающих и сигнальных токов
Какой из нижеперечисленных факторов влияет на эффективность защиты информации от утечки? а) Отношение сигнал/шум на входе приемника сигналов б) Время и затраты на поиск канала утечки в) Демаскирующие признаки носителя информации
Что необходимо сделать для предотвращения утечки информации по техническому каналу? а) Увеличить мощность носителя б) Нейтрализовать преднамеренные и случайные воздействия на источник информации в) Уменьшить информативность признаковой структуры объектов защиты
Что является способом защиты от утечки, возникшей за счет высокочастотного

облучения и ВЧ-навязывания?
а) Генерирование «розового» шума
в) Осуществление периодических проверок на увеличение тока потребления
г) Создание помех в диапазоне от 100 до 1000 мГц
д)Соблюдение размеров контролируемых зон

Что является важнейшим показателем технического канала утечки?
а) Пропускная способность
б) Информативность
в) Длина
г) Среда

Каким показателем характеризуется источник сигнала?
а) Мощность помех
б) Чувствительность
в) Диаграмма направленности излучения
г) Скорость распространения сигнала в среде

Каким из параметров обладает приемник сигналов?
а) Динамический диапазон сигнала
б) Параметр спектра сигнала
в) Пространственная селективность приемной антенны
г) Амплитудно-частотная характеристика

К какому каналу утечки относятся трубы водоснабжения?
а)Параметрический
б) Вибрационный
в) Оптоэлектронный
г) Виброакустический

Что относится к активным способам защиты выделенных помещений?
а) Использование генераторов шума
б) Использование двойных дверей
в) Звукоизоляция помещений

Что из перечисленного относится к портативным подавителям диктофонов?
а) «ANG-2000»
б) «Шумотрон-3»
в) «Шорох»

Какой из перечисленных приборов является генератором шума?
а) «Порог-2М»
б) «Шторм»
в) «Штурм»
г) ST-031M «Пиранья»

Что из перечисленного относится к стационарным подавителям диктофонов?
а) VNG-006
б) «Буран-4»
в) «Шорох»

Какие из перечисленных цепей не формируют потенциально-информативные ПЭМИН?
а) Цепи, формирующие шину данных системной шины компьютера
б) Внутренние цепи блока питания компьютера
в)Цепи, по которым передается видеосигнал от видеоадаптера до электродов электронно-лучевой трубки монитора
г)Цепи, формирующие шину данных системной шины компьютера

Какие из перечисленных цепей не формируют неинформативные ПЭМИ?
а) Цепи, передающие сигналы аппаратных прерываний
б) Цепи, формирующие шину управления и шину адреса системной шины

в) Цепи формирования и передачи сигналов синхронизации г) Внутренние цепи блока питания компьютера д)Цепи, формирующие шину данных внутри микропроцессора
Где не могут возникнуть наводки информативных сигналов? а) В линиях электропитания ЭВМ б) В цепях заземления ЭВМ и ВТСС в)В полипропиленовых трубах систем отопления г)В линиях электропитания и соединительных линиях ВТСС
Что необходимо для возникновения канала утечки? а) Чтобы соединительные линии ВТСС, линии электропитания, посторонние проводники и т.д., выполняющие роль случайных антенн, выходили за пределы контролируемой зоны объекта б) Чтобы расстояние от СВТ до случайной сосредоточенной антенны было более r1, и расстояние до случайной распределённой антенны было более r1 в) Чтобы была возможность непосредственного подключения к случайной антенне только в пределах контролируемой зоны объекта средств разведки ПЭМИН
Каких закладных устройств, внедряемых в СВТ, по виду перехватываемой информации не существует? а) Аппаратные закладки для перехвата изображений, выводимых на экран монитора б) Аппаратные закладки для перехвата информации, хранящейся в оперативной памяти в) Аппаратные закладки для перехвата информации, записываемой на жёсткий диск ПЭВМ г) Аппаратные закладки для перехвата информации, вводимой с клавиатуры ПЭВМ
Каким путем нельзя осуществить перехват информации, обрабатываемой СВТ? а) Перехватом побочных электромагнитных излучений, возникающих при работе СВТ б) Перехватом наводок информативных сигналов с соединительных линий ВТСС и посторонних проводников в)«Низкочастотного облучения» СВТ
На что направлены активные методы защиты? а) На ослабление наводок побочных электромагнитных излучений б) На создание маскирующих пространственных электромагнитных помех в) На исключение (ослабление) просачивания информационных сигналов ТСПИ в цепи электропитания
За счет чего происходит ослабление побочных электромагнитных излучений ТСПИ и их наводок в посторонних проводниках? а) Экранирование и заземление ТСПИ и их соединительных линий б) Фильтрация информационных сигналов в) Пространственное и линейное зашумление
В каких системах, средствах информатизации и связи не может осуществляться фильтрация? а) В высокочастотных трактах передающих и приемных устройств б) В различных сигнальных цепях технических средств в) В цепях электропитания, управления, контроля, коммутации технических средств г) В металлических проводящих конструкциях
На какие группы по способу регистрации можно разить закладные устройства? а) С помощью проводных линий б) С помощью оптического канала в) С помощью микрофона
На какие группы по способу передачи можно разбить закладные устройства? а) С помощью радиоканала б) С помощью пьезокристаллического датчика в) С помощью модуляции отраженного луча от светоотражающих поверхностей

На что направлены пассивные методы защиты акустической информации? а) Создание маскирующих акустических и вибрационных помех б) Создание маскирующих электромагнитных помех в) Ультразвуковое подавление диктофонов в режиме записи г) Обнаружение излучений акустических закладок
На что направлены активные методы защиты акустической информации? а) Ослабление акустических (речевых) сигналов б) Ослабление информационных электрических сигналов в) Электромагнитное подавление диктофонов в режиме записи
Какое устройство используется для локализации установленных закладных устройств? а) «Рубеж» б) «Дельта» в) «Сова»
Какое устройство используется для электромагнитного подавления диктофонов? а) ST-031 «Пиранья» б) NR-90EM в) «Рубеж»
Какая система виброакустической маскировки используется для подавления средств перехвата речевой информации? а) RM-100 б) «Фон-В» в) «УПД»
Для чего предназначен генератор шума ANG-2000? а) Для создания виброакустических помех с целью защиты от проводных и радиомикрофонов б) Для защиты информации от утечки по акустическим и виброакустическим каналам в) Для защиты объектов информатизации 1 категории и противодействия техническим средствам перехвата речевой информации
Чем технические средства расширяют и дополняют возможности человека по добыванию информации? а) Возможностью консервировать информацию на непродолжительное время б) Съемом информации с носителей, которые недоступны органам чувств человека в) Возможностью добычи информации за пределами контролируемой зоны
Что не должно входить в состав отчетных документов о проведении обследования помещения? а) Протоколы изъятия средств съема информации б) Рекомендации по устранению и нейтрализации технических каналов утечки в) Методические рекомендации о степени защищенности объекта
Какое устройство, из перечисленных, предназначено для проверки телефонных коммуникаций? а) Цифровой мультиметр б) OSC-5000 в) NR-900EM

2.3. РАЗДЕЛ 3. ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

На заключительном этапе оформляются результаты работы студентов.

Результаты практики студент обобщает в виде письменного отчета. Отчет по практике является основным документом студента, отражающим,

выполненную им работу во время практики, полученные организационные и технические навыки и знания. Отчет должен быть оформлен и полностью завершен к моменту окончания практики (образец оформления титульного листа отчета см. в приложении 2). Основой отчета являются самостоятельно выполняемые работы студентом в соответствии с программой практики. В отчете описывается методика проведения исследований, отражаются результаты выполнения индивидуального задания. В заключение отчета приводятся краткие выводы о результатах практики, рекомендации по улучшению эффективности деятельности организации. Изложение в отчете должно быть сжатым, ясным и сопровождаться цифровыми данными, схемами, графиками и диаграммами. Цифровой материал необходимо оформлять в виде таблиц. Сложные отчетные и плановые формы и расчеты могут быть оформлены как приложения к отчету с обязательной ссылкой на них в тексте.

Завершающим этапом практики является подведение ее итогов, которое предусматривает выявление степени выполнения студентом программы практики. При оценке итогов работы студента на практике, учитываются содержание и правильность оформления студентом дневника, отзыв руководителя практики от организации, качество ответов на вопросы в ходе защиты.

Примерный перечень вопросов при защите практики:

1. Понятие информационной безопасности. Объект защиты информации. Основные составляющие информационной безопасности. Управление информационной безопасностью.
2. Основные определения и критерии классификации угроз. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.
3. Международный стандарт ISO/IEC 15408.
4. Критерии оценки безопасности информационных систем.Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения.
5. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности.
6. Оценки рисков информационной безопасности.
7. Современные методы и средства анализа и управление рисками информационных систем.
8. Меры обеспечения информационной безопасности.
9. Основные программно-технические меры. Идентификация и аутентификация. Основные понятия.
10. Управление доступом. Основные понятия.
11. Протоколирование и аудит.
12. Шифрование.
13. Контроль целостности. Цифровые сертификаты.

14. Информация как объект правоотношений. Законодательство РФ в области информационной безопасности.
15. Виды и содержание тайн. Законодательная база охраны государственной, коммерческой и служебной тайн.Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных и первоочередные мероприятия по созданию системы защиты персональных данных на предприятии.
16. Виды деятельности, подлежащие лицензированию. Порядок получения лицензии в области защиты информации.
17. Методы и средства инженерной защиты объектов информатизации.
18. Программные и аппаратные средства защиты информации от несанкционированного доступа.

ПРИЛОЖЕНИЕ 1. Форма дневника по практике

ДНЕВНИК

по_____ практике
(вид практики: учебная, производственная (преддипломная), др.)

СТУДЕНТ _____
фамилия, имя, отчество (при наличии)

УЧЕБНОЕ ПОДРАЗДЕЛЕНИЕ _____

_____

КУРС _____ГРУППА_____

Предписание на практику

Студент _____
(фамилия, имя, отчество)

направляется на_____практику
(способ проведения практики: выездная, стационарная)

в г._____на _____
(наименование предприятия)

Срок практики с _____по_____

Руководитель практики от университета

_____
(должность, фамилия, имя, отчество)

М.П. **Руководитель учебного подразделения**_____
(подпись)

М.П. **Прибыл на предприятие**

«_____»_____20_____г._____
(подпись)

Руководитель практики от профильной организации

_____
(должность, фамилия, имя, отчество)

назначен_____
(приказ, распоряжение №, дата)

М.П. **Убыл из предприятия**

«_____»_____20_____г._____
(подпись)

ПАМЯТКА

I. Основные положения по прохождению практики

1. До начала практики руководитель практики от университета: проводит инструктаж по охране труда, сообщает сроки практики, знакомит с перечнем документов, которые должен иметь при себе студент на период практики и выдает:

- дневник с индивидуальным заданием по практике;
- два экземпляра программ практики на группу (один для студентов и один для руководителей практики от профильной организации);
- копию договора о прохождении практики;
- направление на практику;
- назначает старшего по группе из числа студентов;
- направление для поселения в общежитие (в случае необходимости).

2. По прибытии на место прохождения практики студент должен представить договор и направление на практику, ознакомиться с содержанием индивидуального задания, пройти инструктаж по технике безопасности, ознакомиться с рабочим местом, правилами эксплуатации оборудования и уточнить план прохождения практики.

3. Студент во время практики обязан строго соблюдать правила внутреннего распорядка той организации, где проходит практику, требования охраны труда и пожарной безопасности. Обо всех отлучках со своего места практики ставить в известность руководителя практики от предприятия и университета. Выполнять задания, предусмотренные программой практики. Вести дневник по установленной форме.

4. Отчет по практике составляется студентом в соответствии с указаниями программы практики, индивидуальным заданием и дополнительными указаниями руководителей практики от университета и предприятия.

5. Итогом по окончании практики является дифференцированный зачет (зачет с оценкой). Оценка по практике учитывается при подведении итогов общей успеваемости студентов.

II. Правила ведения дневника

1. Дневник является основным документом студента во время прохождения практики.

2. Во время практики студент периодически кратко записывает в дневник все, что им проделано за соответствующий период по выполнению программы практики и индивидуальных заданий.

3. По требованию руководителей практики студент обязан представить дневник на просмотр. Руководители практики подписывают дневник после просмотра, делают свои замечания и дают дополнительные задания.

4.По окончании практики дневник и отчет должны быть просмотрены руководителями практики, составлены отзывы. Дневник должен быть подписан руководителем практики от профильной организации (начальником отдела технического обучения, главным инженером или другими ответственными за практику лицами) и руководителем практики от университета.

5.Защита отчета по практике проводится на кафедре в конце практики.

Рабочий график(план) проведения практики

Сроки работы	Цех, отдел или лаборатория и рабочее место студента

Подписи:
Руководитель практики от университета _____

Руководитель практики от профильной организации _____

Индивидуальные задания на период практики

Содержание индивидуального задания и планируемые результаты

Подписи:
Руководитель практики от университета _____
Согласовано
Руководитель практики от профильной организации _____

С требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка в _____

(наименование организации, рабочего места)

Ознакомлен студент_____

(подпись, ФИО, дата)

Инструктаж провел руководитель практики от профильной организации

_____

(подпись, ФИО, дата)

Дата	Рабочие записи

Замечания руководителя практики от университета по ходу практики

Отзыв руководителя практики от профильной организации о практике студента

Рекомендуемая оценка_____

Руководитель практики от профильной организации

М.П. **_____**

«_____»_____ 20_____г.

Заключение руководителя практики от университета о практике студента

Руководитель практики от университета

Зачетная оценка по практике_____

Подпись_____ «____»_____20___г.

ПРИЛОЖЕНИЕ 2.
Примерный образец титульного листа отчета по практике

УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет математики, информационных и авиационных технологий
Кафедра информационной безопасности и теории управления

ОТЧЕТ
ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

Специальность _____
(шифр и название специальности)

Специализация: _____

Студент (ка) __ _ курса Группа _____

_____ _____
ФИО полностью подпись

Руководитель практики от УлГУ: _____ _____
(должность, ФИО) подпись

УЛЬЯНОВСК 20__