МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент гр.
С8118-10.05.01ммзи
_____ Ялынычев Д.В.
(подпись)

Отчет защищен с оценкой
_____
_____ С.С. Зотов
(подпись) (И.О. Фамилия)
« 31 » июля 2021 г.

Руководитель практики
Должность на предприятии
_____ _____
(подпись) (И.О. Фамилия)

Регистрационный № _____
« 31 » июля 2021 г.

_____ Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.
на предприятии
АО «Изумруд»

г. Владивосток
2021

Характеристика

Выдана студенту 3 курса, специальности «Компьютерная безопасность», специализация «Математические методы защиты информации», Ялынычеву Денису Владимировичу.

Ялынычев Денис Владимирович, в период с 19.07.2021 по 31.07.2021 года, проходил учебную (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практику на предприятии АО «Изумруд».

За время прохождения практики Денис проявил усердие, тягу к знаниям, огромное желание и трудолюбие, а также неподдельный интерес к изучению материала. Приходил на консультацию вовремя с перечнем вопросов, с подробным и исчерпывающим описанием о текущем состоянии практики, со списком отмеченных задач. Внимательно изучал предложенные материалы и литературу на интересующую тематику.

Ялынычев Д.В. полностью выполнил предусмотренную программу практики, продемонстрировал умения самостоятельно решать практические вопросы, применяя теоретическую базу, полученную в учебный период, а также при самостоятельном обучении.

По итогам прохождения практики Денис изучил все аспекты работы предприятия, работал с профессиональным оборудованием и получил основные теоретические знания в сфере обеспечения защиты информации.

При выполнении поставленных задач Ялынычев Д.В. характеризуется инициативностью, сообразительностью и ответственностью.

Должность на предприятии _____ ФИО

ДНЕВНИК СТУДЕНТА

Дата	Рабочее место	Краткое содержание выполняемых работ	Отметки руководителя
19.07.21 – 20.07.21	АО «Изумруд»	Изучение деятельности предприятия и общение с действующими специалистами, знакомство с рабочим местом и функциональными обязанностями	
21.07.21 – 26.07.21	АО «Изумруд»	Знакомство с организацией производства и технологией выполнения работ	
27.07.21 – 28.07.21	АО «Изумруд»	Работа с профессиональным оборудованием	
29.07.21 – 31.07.21	АО «Изумруд»	Написание отчёта по проделанной работе	

Студент _____Ялынычев Д.В._____

подпись Ф.И.О.

Руководитель практики от предприятия _____

подпись Ф.И.О.

Содержание

Задание на практику

- Изучение деятельности предприятия и общение с действующими специалистами.
- Знакомство с рабочим местом и функциональными обязанностями.
- Знакомство с организацией производства и технологией выполнения работ.
- Работа с профессиональным оборудованием.

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на предприятии АО «Изумруд» в период с 19 июля 2021 года по 31июля 2021 года.

Цель практики - повышение уровня и качества подготовки студентов за счет ознакомления с профессией. Студент знакомится с реальной практической деятельностью предприятия, что позволяет ему понять специфику своей будущей профессии.

Задачи практики:

- изучение специфики деятельности предприятия;
- формирование профессиональных навыков;
- приобретение опыта работы по специальности;
- приобретение опыта работы в коллективе;
- знакомство с рабочим местом и функциональными обязанностями;
- работа с профессиональным оборудованием.

1.1 Деятельность предприятия и технология выполнения работ

Акционерное общество «Изумруд» – российское предприятие, разработчик и производитель корабельных радиолокационных систем, предназначенных для автоматического управления стрельбой корабельной зенитной артиллерией.

Завод «Изумруд» был создан 31 декабря 1965 года. Его статус, цели и задачи, функции и полномочия были определены Приказом Министра радиопромышленности СССР № 306 от 31.12.1965 г., по которому был открыт завод «Электродеталь», в последствии переданный для управления в Министерство судостроительной промышленности СССР. 12 января 1972 года предприятие переименовано в завод «Изумруд», а в 1994 году в Акционерное общество «Изумруд».

С 2007 года завод входит в состав АО «Концерн «Моринформсистема-Агат» наряду с другими предприятиями, формирующими практически весь спектр интеллектуальной начинки кораблей и подводных лодок.

1.2 Описание рабочего места и функциональных обязанностей

Рабочее место, где проходила практика, находилось в офисе «Отдела по защите информации», среди работающих сотрудников.

Функциональные обязанности:

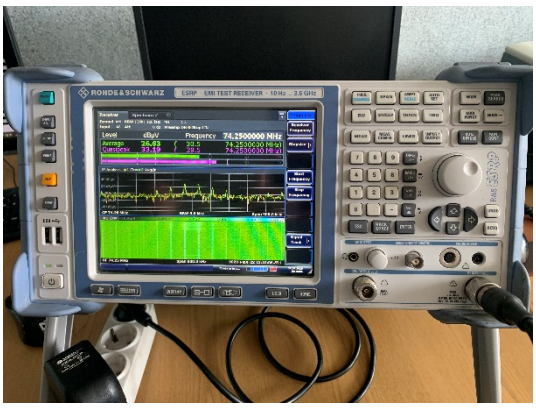
- изучение работы предприятия:

  Предприятие АО «Изумруд» затрагивает множество областей в сфере производства:

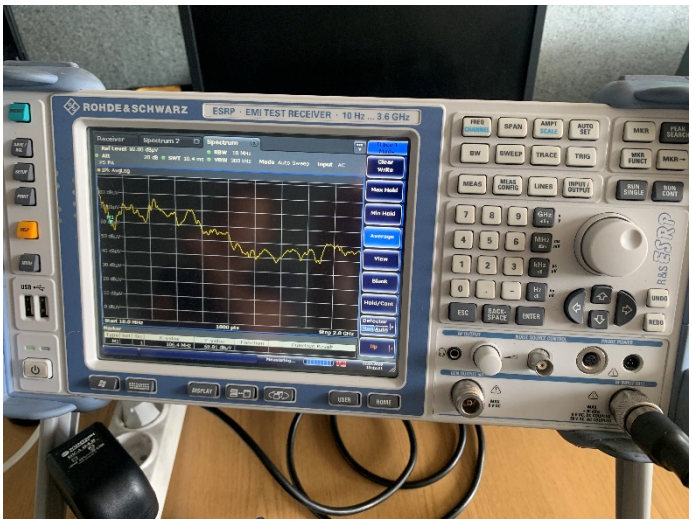
  - Заготовительное производство;
  - Металлообрабатывающее производство;
  - Гальваническое производство;
  - Покрасочное производство;
  - Производство изделий из неметаллов;
  - Производство печатных плат;
  - Защита информации:
    - Оказание услуг в области защиты информации: проведение аттестации информационных систем (АС, АСУТП, ИСПДн, ГИС) и помещений.
    - Оказание консультативных услуг по выполнению организационных и технических требований законодательства Российской Федерации в области защиты информации.

- ознакомление с профессиональным оборудованием:

  В процессе прохождения практики меня познакомили с работой органа по аттестации объектов информатизации. Продемонстрировали оборудования, при помощи которых проводится аттестация. Объяснили их принцип работы.

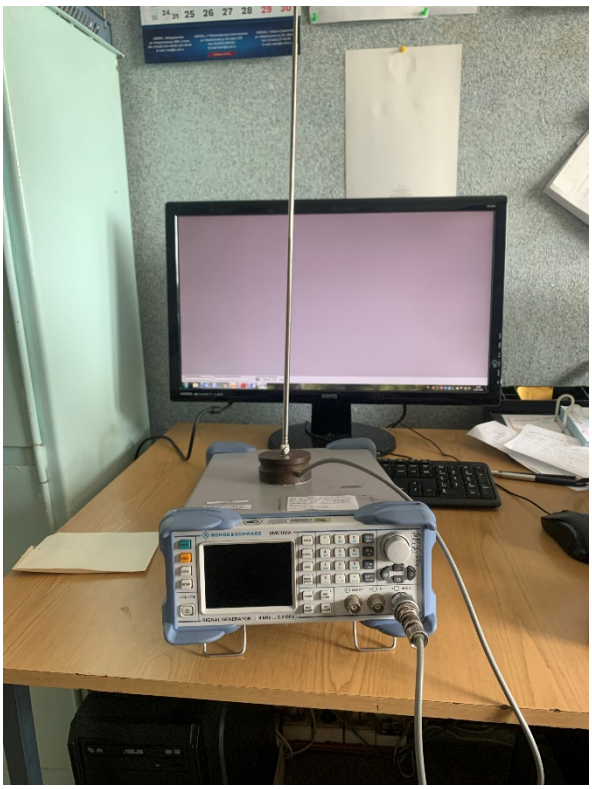


Поиск информативного сигнала



Замер генератора шума. На примере Сонаты Р3.1

Замер акустических сигналов



Генератор сигнала

В частности, мне рассказали про измерительный комплекс для технического контроля состояния акустической защищенности помещений и измерительный комплекс Побочных ЭлектроМагнитных Излучений и Наводок (ПЭМИН), обучили их развертыванию и показали проведение измерений:

1) Технический контроль состояния акустической защищенности помещения проводится в целях документального подтверждения реальной возможности утечки акустической информации из проверяемого помещения во время проведения в нем закрытых мероприятий.

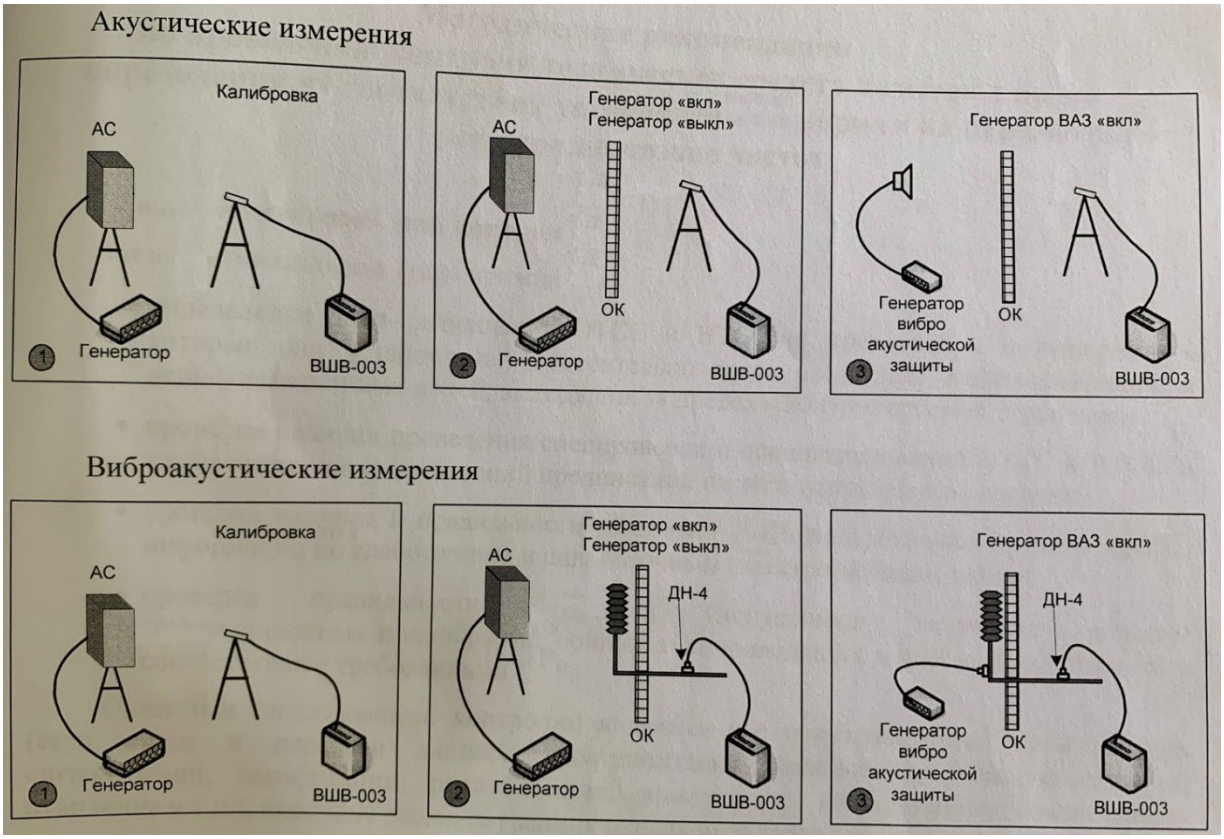
   При оценке мероприятий по защите помещений от утечки акустической речевой информации учитываются следующие возможные каналы утечки информации:

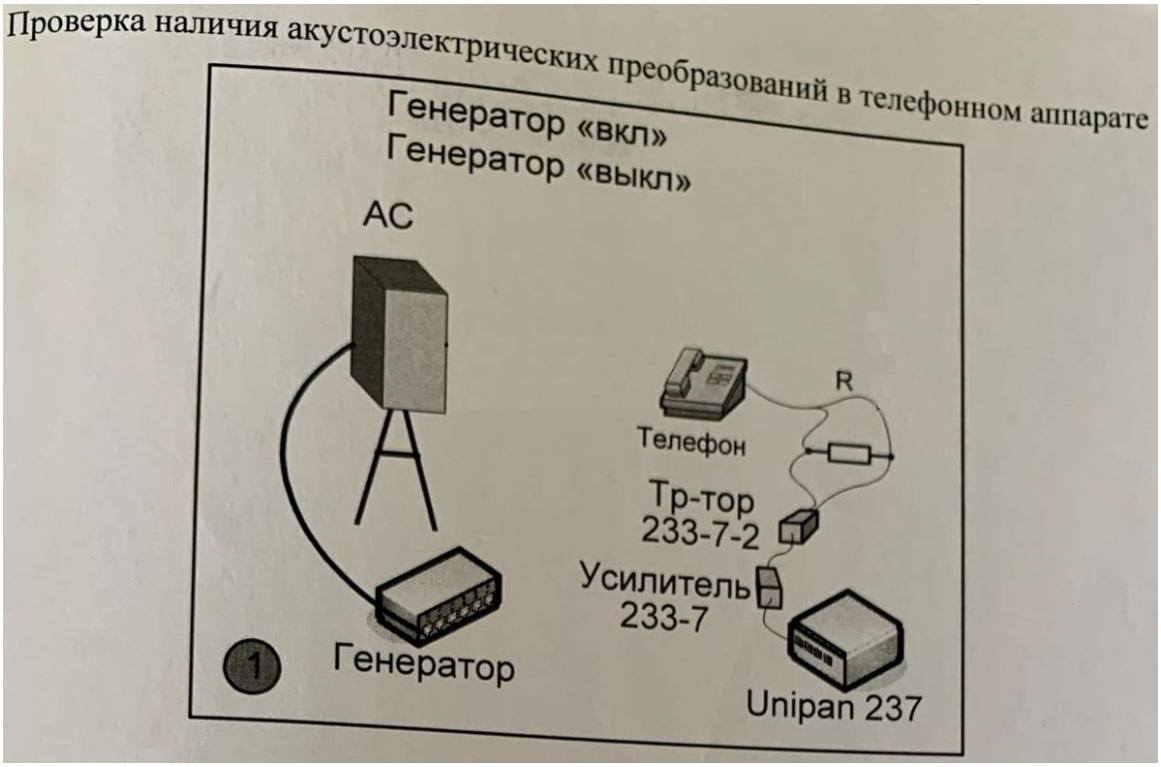
   - акустическое излучение информативного речевого сигнала;

- электрические сигналы, возникающие посредством преобразования из акустического за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации (акустоэлектрические преобразования);
- вибрационные сигналы, возникающие посредством преобразования из акустического при воздействии его на строительные конструкции и инженерно-технические коммуникации помещений;
- излучения случайных источников (паразитных генераторов), модулированные звуковым сигналом (электроакустические преобразования).

Измерительный комплекс должен содержать:

- генератор шума;
- усилитель мощности;
- акустический излучатель;
- измерительный микрофон;
- вибродатчик (акселерометр);
- измеритель шума и вибраций (шумомер);


Акустические измерения
Калибровка
АС
Генератор
ВШВ-003
1
Генератор «вкл»
Генератор «выкл»
АС
ОК
Генератор
ВШВ-003
2
Генератор ВАЗ «вкл»
Генератор вибро акустической защиты
ОК
ВШВ-003
3
Виброакустические измерения
Калибровка
АС
Генератор
ВШВ-003
1
Генератор «вкл»
Генератор «выкл»
АС
ДН-4
ОК
Генератор
ВШВ-003
2
Генератор ВАЗ «вкл»
ДН-4
Генератор вибро акустической защиты
ОК
ВШВ-003
3


Проверка наличия акустоэлектрических преобразований в телефонном аппарате
Генератор «вкл»
Генератор «выкл»
АС
R
Телефон
Тр-тор
233-7-2
Усилитель
233-7
Unipan 237
1
Генератор

2) Измерительный комплекс ПЭМИН должен содержать:

- Приемник измерительный;
- Антенна измерительная дипольная;
- Антенна измерительная рамочная;
- Токосъемник измерительный;

Вспомогательное оборудование:

- Генератор сигналов
- Антенна штыревая;

Схема инструментального контроля ПЭМИН:

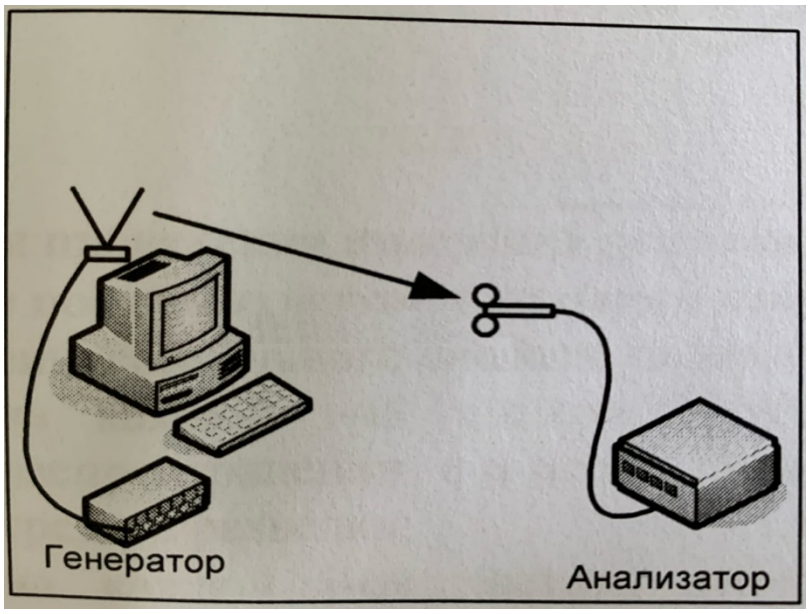
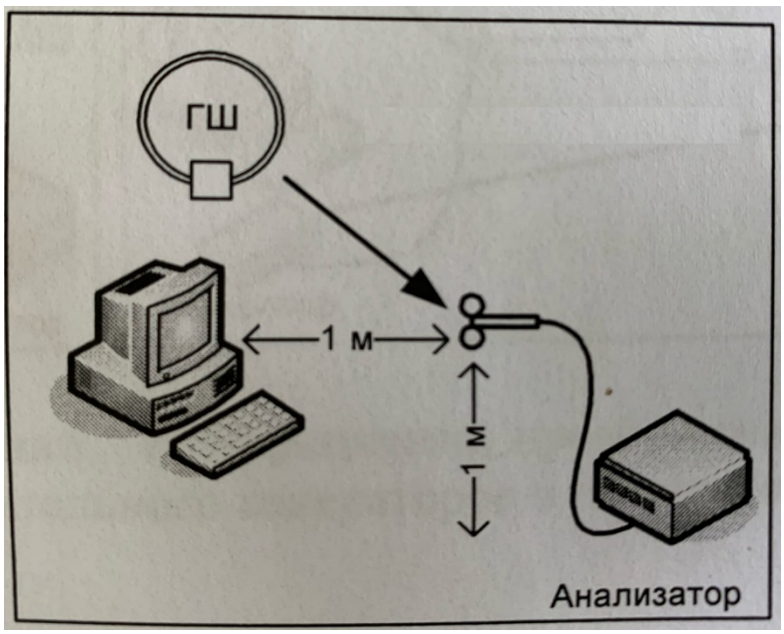


Схема проверки Генератора Шума (ГШ):



1.3 Описание технологического процесса оказания услуг безопасности информации

Технологический процесс оказания услуг безопасности информации состоит из пяти этапов:

1) Заключение договора, в котором уточняются критерии обеспечения безопасности информации.
2) Анализ помещений.
3) Установление необходимого оборудования и средств защиты информации (СЗИ).
4) Измерение ПЭМИН и определение КЗ (контролируемой зоны).
5) Сдача объекта.

1) Фирмы, для которых необходимо осуществить мероприятия и оказание услуг в области защиты информации: провести контроль защищённости информации; осуществить аттестацию средств и систем на соответствие требованиям по защите информации, обращаются в отдел по защите информации АО «Изумруд». После этого сотрудник отдела едет на обследование объекта информатизации к заказчику и проверяет на соответствие требованиям руководящих документов. Далее, если объект информатизации соответствует требованиям, то начинается процедура заключения договора. В противном случае, если объект не соответствует требованиям, то заказчику выдаются рекомендации по устранению недочётов, после устранения которых, начинается процедура заключения договора.

Договор состоит из следующих пунктов:

1. Предмет договора
2. Срок оказания услуг и иных положений
3. Стоимость и порядок расчёта
4. Условия и порядок оказания услуг
5. Права и обязанности сторон
6. Ответственность сторон и порядок разрешения споров

7. Форс-мажор
8. Антикоррупционная оговорка
9. Заключительные положения
10. Местонахождение, почтовые адреса, реквизиты и подписи сторон

Также в договоре идёт описание оказываемых услуг. Например, аттестация АРМ:

- Предварительное обследование объекта с выездом к заказчику:
  - выявление возможных каналов утечки информации;
  - анализ обстановки;
  - составление программы и методики аттестации.
- Анализ исходных данных:
  - анализ циркулирующей информации, определение категории и класса защиты объекта;
  - анализ состава и характеристик технических (ОТСС, ВТСС), программных средств;
  - изучение технологического процесса обработки и хранения защищаемой информации;
  - анализ информационных потоков;
  - определение угроз несанкционированного доступа к информации.
- Экспертиза эксплуатационно-распорядительной документации, имеющейся на объекте.
- Инструментальная оценка защищенности объекта от утечки по каналам ПЭМИ.
- Инструментальная оценка защищенности объекта за счет наводок на линии ВТСС.
- Инструментальная оценка защищенности объекта от утечки по цепям заземления и электропитания.
- Оценка эффективности применяемых средств защиты (от утечки по каналу ПЭМИ, по цепям заземления и электропитания и линиям ВТСС)

- Оценка состояния организации работ и выполнения организационно – режимных требований по защите информации.
- Проверка уровня подготовки персонала, отвечающего за обеспечение требований по защите информации на объекте.
- Проверка и испытания АС на соответствие требованиям по защите информации от несанкционированного доступа.
- Оформление документов по результатам аттестационных испытаний с выдачей аттестата соответствия на объект информатизации.
- Настройка системы защиты информации от НСД.
- Доработка комплекта организационной и технической документации.

2) При анализе помещения необходимо определить каналы утечки информации.

Возможные каналы утечки информации в помещении:

1. Акустический (акустическое излучение информативного речевого сигнала).
2. Виброакустический (вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации помещения).
3. Акустоэлектрические преобразования:
   – электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счёт «микрофонного эффекта» и распространяющиеся по проводам и линиям передачи информации;
   – радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах технических средств;
4. Внедрения электронных устройств перехвата информации.

Следующие услуги могут быть включены в аттестацию помещения:

- Предварительное обследование объекта:
  - выявление возможных каналов утечки информации;
  - анализ обстановки;
  - составление программы и методики аттестации.
- Анализ исходных данных:
  - анализ циркулирующей информации, определение категории объекта;
  - анализ информационных потоков.
- Экспертиза эксплуатационно-распорядительной документации, имеющейся на объекте.
- Инструментальный контроль защищенности помещения по акустическому каналу.
- Оценка эффективности применяемых средств активной защиты по акустическому каналу.
- Оценка состояния организации работ и выполнения организационно-режимных требований по защите информации.
- Оформление заключения по результатам аттестационных испытаний с выдачей аттестата соответствия на объект информатизации.

Пример быстрого анализа опасности

Объект – помещение. Вид разведки – акустическая речевая.

Канал утечки	Ограждающие конструкции	Угол направления на средство съёма, градусы	Расстояние до места возможного перехвата, м	Актуальность канала
- виброакустический (аппаратура лазерного зондирования отражающих поверхностей)	- оконные проёмы	0	50	Актуально
Канал утечки	Ограждающие конструкции	Наличие мест возможного перехвата за пределами КЗ, да – нет	Расстояние до места возможного перехвата, м	Актуальность канала
- акустический (направленные микрофоны)	- оконные проёмы - стены - вентиляция	Да Да Нет	50 50 0	Актуально Актуально Неактуально
Канал утечки	Ограждающие конструкции	Возможность подхода, да – нет	Расстояние до места возможного перехвата, м	Актуальность канала
- акустический (непреднамеренное прослушивание)	- дверные проёмы - стены - вентиляция - окна	Да Да Нет Нет	- - - -	Актуально Актуально Неактуально Неактуально
Канал утечки	Коммуникации или ограждающие конструкции	Наличие выхода за пределы КЗ, да – нет	Расстояние до КЗ, м	Актуальность канала
- виброакустический	- система отопления - водопровод - стены, окна	Да Нет Нет	- - -	Актуально Неактуально Неактуально
Канал утечки	Линии	Наличие выхода за пределы КЗ, да – нет	Расстояние до КЗ, м	Актуальность канала
- акустоэлектрический (по проводам и линиям)	- линии электропитания и заземления - телефонные линии - линии сигнализации - линии радиотрансляции - линии часофикации	Да Да Нет Нет Нет	- - - - -	Актуально Актуально Неактуально Неактуально Неактуально
Канал утечки	ОТСС, ВТСС	Наличие предписания на эксплуатацию в помещении, да - нет	Расстояние до КЗ, м	Актуальность канала
- акустоэлектрический (радиоизлучения модулированных генераторов)	- ПЭВМ - кондиционер - телевизор - радиоприёмник - проектор - холодильник	Нет Да Нет Нет Нет Да	- - - - - -	Актуально Неактуально Актуально Актуально Актуально Неактуально
Канал утечки	ОТСС, ВТСС	Наличие заключения о спецпроверке, да – нет	Расстояние до КЗ, м	Актуальность канала
- акустоэлектрический (специальные электронные устройства перехвата информации – закладные устройства)	- технические средства иностранного производства	Нет	-	Актуально

3) В зависимости от того, какие средства защиты требуется установить для АРМ:

- СЗИ от НСД;
- Генераторы шума;
- Средство доверенной загрузки. Например, ПАК «Соболь» - сертифицированный аппаратно-программный модуль доверенной загрузки (АПМДЗ) с поддержкой UEFI. Предназначен для:
  - защиты конфиденциальной информации, персональных данных, гостайны;
  - предотвращения доступа неавторизованных пользователей к информации, обрабатываемой на компьютере;
  - информирования администратора комплекса всех важных событиях ИБ;
  - предоставления случайных чисел прикладному ПО.
- Антивирусные средства;
- АРМ должен пройти спецпроверку, специсследования и иметь предписания на эксплуатацию.

Для помещения:

- Система активной акустической и вибрационной защиты акустической речевой информации (например, Соната-АВ модель 4Б). При обследовании определяется канал утечки, и на основании этого устанавливаются составные части этой системы (для Сонаты-АВ модели 4Б: блок электропитания и управления, генератор-акустоизлучатель, генератор-вибровозбудитель, размыкатель телефонной линии, размыкатель слаботочной линии, размыкатель линии Ethernet)
- Всё оборудование иностранного или совместного производства, устанавливаемое в помещениях, должно пройти спецпроверку, специсследования и иметь предписания на эксплуатацию.

4) Контроль защищённости осуществляется с целью предупреждения возможности получения аппаратурой разведки Побочных ЭлектроМагнитных Излучений и Наводок (ПЭМИН) информации, циркулирующей на защищаемом от

разведки ПЭМИН объекте, оценки состояния, полноты и своевременности проведения мероприятий по противодействию разведке ПЭМИН.

В процессе контроля защищённости на объекте проверяются все основные технические средства от утечки за счёт ПЭМИН, а также вспомогательные технические средства, имеющие в своём составе генераторы, радиоизлучения которых могут быть непреднамеренно промоделированы сигналом, несущим защищаемую информацию.

Различается два вида контроля защищённости объектов от разведки ПЭМИН:

- аттестационный контроль;
- периодический (эксплуатационный) контроль.

Аттестационный контроль проводится при создании объекта информатизации, а также после его реконструкции или модернизации.

Периодический (эксплуатационный) контроль проводится в процессе эксплуатации объекта. Периодичность такого контроля регламентируется руководящим документом.

При проведении контроля защищённости проверяются параметры, которые характеризуют защищённость технических средств или объекта в целом, в соответствии с установленной категорией объекта защиты.

Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. КЗ определяется для каждого объекта информатизации. Её можно определить после обследования объекта информатизации.

5) После проверки объектов информатизации на соответствие всем требованиям происходит оформление аттестационных документов. Оформляются протоколы аттестационных испытаний на соответствие требованиям по ЗИ. По результатам аттестационных испытаний оформляется заключение. На основании заключения аттестационных испытаний выдаётся аттестат соответствия, подписывается с двух сторон акт выполненных работ и договор закрывается.

Заключение

Для достижения поставленной цели - повышение уровня и качества подготовки студентов за счет ознакомления с профессией - в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики познакомился с нормативной базой по информационной безопасности и аспектами работы в отделе по защите информации.

Благодаря общению с сотрудниками было получено представление о работе, связанной с моей специальностью.

В ходе прохождения практики познакомился с профессиональным оборудованием и получил общее представление о работе предприятия, специализирующегося на безопасности информации.

В результате прохождения практики все задачи были выполнены, а цель достигнута. Кроме того, приобретен профессиональный опыт в сфере информационной безопасности.

Нормативная база

1) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», устанавливающих основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн;
2) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3) Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
4) Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
5) Приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 г. Москва «Об утверждении Состава и содержания организационных и технический мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
6) Постановление Правительства РФ от 21.03.2012 № 211 (ред. от 06.09.2014) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

7) Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
8) Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
9) Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».