С. Н. Новиков

Кафедра «БиУТ»

Системы контроля и управления доступом

*Методические указания по выполнению*

Контрольная работа

*ТЕМА:* Разработка системы контроля и управления доступа на стадионе.

Новосибирск 2018

Содержание

[1 СТРУКТУРА КОНТРОЛЬНОЙ РАБОТЫ 3](#_Toc524084521)

[2 ПОРЯДОК ВЫПОЛНЕНИЯ КОНТРОЛЬНОЙ РАБОТЫ 4](#_Toc524084522)

[2.1 Выбор темы 4](#_Toc524084523)

[2.2 Составление плана подготовки контрольной работы 4](#_Toc524084524)

[2.3 Подбор, изучение, анализ и обобщение материалов по выбранной теме 4](#_Toc524084525)

[2.4 Разработка содержания контрольной работы 5](#_Toc524084526)

[2.4.1 Разработка введения 5](#_Toc524084527)

[2.4.2 Разработка основной части контрольной работы 8](#_Toc524084528)

[2.4.3 Разработка заключения 9](#_Toc524084529)

[2.4.4 Составление списка источников и литературы 10](#_Toc524084530)

[3 ОБЩИЕ ПРАВИЛА ОФОРМЛЕНИЯ КОНТРОЛЬНЫХ РАБОТ 11](#_Toc524084531)

[3.1 Требования к лингвистическому оформлению контрольной работы 11](#_Toc524084532)

[ПРИЛОЖЕНИЕ 1. Перечень тем контрольной работы 15](#_Toc524084533)

[ПРИЛОЖЕНИЕ 2. Пример разработки введения контрольной работы 17](#_Toc524084534)

[ПРИЛОЖЕНИЕ 3. Пример оформления списка источников и литературы 19](#_Toc524084535)

[ПРИЛОЖЕНИЕ 4. Пример выполнения глав контрольной работы 21](#_Toc524084536)

# 1 СТРУКТУРА КОНТРОЛЬНОЙ РАБОТЫ

По содержанию контрольная работа может носить конструкторский или технологический характер. По структуре контрольная работа состоит из пояснительной записки и практической (графической) части.

**Пояснительная записка контрольной работы конструкторского характера** включает в себя:

* титульный лист;
* задание;
* содержание;
* аннотацию с кратким содержанием работ, выполненных в курсовом проекте;
* введение, в котором раскрывается актуальность и значение темы, формулируется цель;
* описательную часть, в которой приводится анализ современных защищенных телекоммуникационных систем (технических средств защиты информации); описание методов установки, настройки оборудования телекоммуникационных систем; мероприятия по обслуживанию технических средств защиты информации; поиск неисправностей технических средств защиты информации и их устранение;
* заключение, в котором содержатся выводы и рекомендации относительно возможностей использования материалов работы;
* список источников и литературы;
* приложения.

Практическая часть контрольной работы может быть представлена чертежами, схемами, графиками, диаграммами, наглядными изображениями, слайд-презентациями или другими продуктами творческой деятельности в соответствии с выбранной темой.

Объем пояснительной записки контрольной работы должен быть не менее 25 страниц печатного текста, объем графической части 1-2 листа.

# 2 ПОРЯДОК ВЫПОЛНЕНИЯ КОНТРОЛЬНОЙ РАБОТЫ

## 2.1 Выбор темы

Выбор темы контрольной работы определяется последней цифрой номера Вашего пароля (Приложение 1).

## 2.2 Составление плана подготовки контрольной работы

В самом начале работы очень важно составить план выполнения контрольной работы (Приложение 2).

## 2.3 Подбор, изучение, анализ и обобщение материалов по выбранной теме

Прежде, чем приступить к разработке содержания контрольной работы, очень важно изучить различные источники (законы, ГОСТы, ресурсы Интернет, учебные издания и др.) по заданной теме.

Процесс изучения учебной, научной, нормативной, технической и другой литературы требует внимательного и обстоятельного осмысления, конспектирования основных положений, кратких тезисов, необходимых фактов, цитат, что в результате превращается в обзор соответствующей книги, статьи или других публикаций.

От качества Вашей работы на данном этапе зависит качество работы по факту её завершения.

**Внимание!** При изучении различных источников очень важно все их фиксировать сразу. В дальнейшем данные источники войдут у Вас в список источников и литературы.

Практический совет: создайте в своем компьютере файл «Источники и литература по КП» и постепенно туда вписывайте исходные данные любого источника, который Вы изучали по теме контрольной работы. Чтобы не делать работу несколько раз, внимательно изучите требования к составлению списка источников и литературы (Приложение 3).

Результат этого этапа контрольной работы – это сформированное понимание предмета исследования, логически выстроенная система знаний сущности содержания и структуры исследуемой проблемы.

Итогом данной работы может стать необходимость отойти от первоначального плана, что, естественно, может не только изменить и уточнить структуру, но качественно обогатить содержание контрольной работы.

## 2.4 Разработка содержания контрольной работы

Контрольная работа имеет ряд структурных элементов: введение; аналитический обзор; описание выбранного варианта установки, настройки инженерно-технического оборудования; особенности эксплуатации технического средства защиты информации; диагностика, поиск и устранение неисправностей; техника безопасности и охрана труда; заключение; графическая часть.

### 2.4.1 Разработка введения

Во-первых, во введении следует обосновать актуальность избранной темы контрольной работы, раскрыть ее теоретическую и практическую значимость, сформулировать цели и задачи работы (Приложение 2).

Во-вторых, во введении, а также в той части работы, где рассматривается теоретический аспект данной проблемы, автор должен дать, хотя бы кратко, обзор источников и литературы, изданной по этой теме.

Введение должно подготовить читателя к восприятию основного текста работы. Оно состоит из обязательных элементов, которые необходимо правильно сформулировать. В первом предложении называется тема курсовой работы.

**Актуальность исследования** рассматривается с позиций современного состояния технической защиты информации (инженерно-технической защиты). В данном пункте необходимо раскрыть суть исследуемой проблемы и показать степень ее проработанности в различных статьях специальных журналов. Здесь же можно перечислить источники информации, используемые для исследования.

**Цель исследования** заключаться в решении исследуемой проблемы путем ее анализа и практической реализации. Цель всегда направлена на объект.

**Проблема исследования** показывает осложнение, нерешенную задачу или факторы, мешающие её решению. Определяется 1 - 2 терминами.

**Объект исследования** предполагает работу с понятиями. В данном пункте дается определение явлению, на которое направлена исследовательская деятельность. Объектом может быть личность, среда, процесс, структура, хозяйственная деятельность предприятия (организации).

**Предмет исследования -** здесь необходимо дать определение планируемым к исследованию конкретным свойствам объекта или способам изучения явления. Предмет исследования направлен на практическую деятельность и отражается через результаты этих действий.

**Гипотеза исследования**. Возможная структура гипотезы:

* утверждение значимости проблемы.
* догадка (свое мнение) «Вместе с тем…».
* предположение «Можно...».
* доказательство «Если...».

**Задачи исследования** соотносятся с гипотезой. Определяются они, исходя из целей работы. Формулировки задач необходимо делать как можно более тщательно, поскольку описание их решения должно составить содержание глав и параграфов работы. Как правило, формулируются 3-4 задачи.

**Перечень рекомендуемых задач:**

1. «На основе теоретического анализа литературы разработать...» (ключевые понятия, основные концепции).
2. «Определить... » (выделить основные условия, факторы, причины, влияющие на объект исследования).
3. «Раскрыть... » (выделить основные условия, факторы, причины, влияющие на предмет исследования).
4. «Разработать... » (средства, условия, формы, программы).
5. «Апробировать…» (что разработали) и дать рекомендации...

**Методы исследования** - дается краткое перечисление методов исследования, через запятую, без обоснования.

**Теоретическая и практическая значимость исследования** не носит обязательного характера. Наличие сформулированных направлений реализации полученных выводов и предложений придает работе большую практическую значимость.

При написании можно использовать следующие фразы: результаты исследования позволят осуществить...; будут способствовать разработке...; позволят совершенствовать….; представляют интерес для ….(*указать специалистов, которые при решении профессиональных задач могут использовать результаты проведенного исследования).*

**Структура работы –** это завершающая часть введения. В завершающей части в назывном порядке перечисляются структурные части проекта, например: «Структура работы соответствует логике исследования и включает в себя введение, теоретическую часть, практическую часть, заключение, список литературы, 5 приложений».

Здесь допустимо дать развернутую структуру контрольной работы и кратко изложить содержание глав. (Чаще содержание глав контрольной работы излагается в заключении).

Таким образом, введение должно подготовить к восприятию основного текста работы.

Краткие комментарии по формулированию элементов введения представлены в таблице 1.



### 2.4.2 Разработка основной части контрольной работы

Основная часть обычно состоит из двух разделов: в первом содержатся теоретические основы темы; дается история вопроса, уровень разработанности вопроса темы в теории и практике посредством сравнительного анализа литературы и интернет - источников.

В теоретической части рекомендуется провести аналитический обзор методов установки, настройки оборудования телекоммуникационной системы, технической литературе и интернет-источниках. Теоретическая часть предполагает анализ объекта исследования и должна содержать ключевые понятия, историю вопроса, уровень разработанности проблемы в теории и практике. Излагая содержание публикаций других авторов, необходимо *обязательно* давать ссылки на них с указанием номеров страниц этих информационных источников. Исходя из темы контрольной работы, студент проводит рассмотрение принципа работы, назначение, функциональные особенности аналогичных инженерно-технической защиты информации. В данном разделе также рассматриваются достоинства и недостатки приведенных устройств. На этом этапе также может быть рассмотрен принцип построения аналогичных схем и их сравнение.

Вторым разделом является практическая часть, которая должна носить сугубо прикладной характер. В ней необходимо описать конкретный объект исследования, привести результаты практических результатов и направленное их использования, а также сформулировать направления совершенствования.

### 2.4.3 Разработка заключения

Обращаем Ваше внимание, что по окончанию исследования подводятся итоги по теме. Заключение носит форму синтеза полученных в работе результатов. Его основное назначение - резюмировать содержание работы, подвести итоги проведенного исследования. В заключении излагаются полученные выводы, определяется их соотношение с целью исследования, конкретными задачами, гипотезой, сформулированными во введении.

Проведенное исследование должно подтвердить или опровергнуть гипотезу исследования. В случае опровержения гипотезы, даются рекомендации по возможному совершенствованию деятельности в свете исследуемой проблемы.

### 2.4.4 Составление списка источников и литературы

В список источников и литературы включаются источники, изученные Вами в процессе подготовки работы, в т.ч. те, на которые Вы ссылаетесь в тексте контрольной работы.

**Внимание!** Список источников и литературы оформляется в соответствии с правилами, предусмотренными государственными стандартами (Приложение 3).

Список источников и литературы должен содержать 20 – 25 источников (не менее 10 книг и 10-15 материалов периодической печати), с которыми работал автор контрольной работы.

Список источников и литературы включает в себя:

* нормативные правовые акты;
* научную литературу и материалы периодической печати;
* практические материалы.

Источники размещаются в алфавитном порядке. Для всей литературы применяется сквозная нумерация.

При ссылке на источники и литературу в тексте контрольной работы следует записывать не название книги (статьи), а присвоенный ей в указателе “Список источников и литературы” порядковый номер в квадратных скобках. Ссылки на источники и литературу нумеруются по ходу появления их в тексте записки. Применяется сквозная нумерация.

# 3 ОБЩИЕ ПРАВИЛА ОФОРМЛЕНИЯ КУРСОВЫХ ПРОЕКТОВ

## 3.1 Требования к лингвистическому оформлению контрольной работы

Контрольная работа должен быть написан логически последовательно, литературным языком. Повторное употребление одного и того же слова, если это возможно, допустимо через 50 – 100 слов. Не должны употребляться как излишне пространные и сложно построенные предложения, так и чрезмерно краткие лаконичные фразы, слабо между собой связанные, допускающие двойные толкования и т. д.

При написании контрольной работы не рекомендуется вести изложение от первого лица единственного числа: «я наблюдал», «я считаю», «по моему мнению» и т. д. Корректнее использовать местоимение «мы». Допускаются обороты с сохранением первого лица множественного числа, в которых исключается местоимение «мы», то есть фразы строятся с употреблением слов «наблюдаем», «устанавливаем», «имеем». Можно использовать выражения «на наш взгляд», «по нашему мнению», однако предпочтительнее выражать ту же мысль в безличной форме, например:

1. *изучение педагогического опыта свидетельствует о том, что …,*
2. *на основе выполненного анализа можно утверждать …,*
3. *проведенные исследования подтвердили…;*
4. *представляется целесообразным отметить;*
5. *установлено, что;*
6. *делается вывод о…;*
7. *следует подчеркнуть, выделить;*
8. *можно сделать вывод о том, что;*
9. *необходимо рассмотреть, изучить, дополнить;*
10. *в работе рассматриваются, анализируются...*

При написании контрольной работы необходимо пользоваться языком научного изложения. Здесь могут быть использованы следующие слова и выражения:

1. для указания на последовательность развития мысли и временную соотнесенность:
* *прежде всего, сначала, в первую очередь;*
* *во – первых, во – вторых и т. д.;*
* *затем, далее, в заключение, итак, наконец;*
* *до сих пор, ранее, в предыдущих исследованиях, до настоящего времени;*
* *в последние годы, десятилетия;*
1. для сопоставления и противопоставления:
* *однако, в то время как, тем не менее, но, вместе с тем;*
* *как…, так и…;*
* *с одной стороны…, с другой стороны, не только…, но и;*
* *по сравнению, в отличие, в противоположность;*
1. для указания на следствие, причинность:
* *таким образом, следовательно, итак, в связи с этим;*
* *отсюда следует, понятно, ясно;*
* *это позволяет сделать вывод, заключение;*
* *свидетельствует, говорит, дает возможность;*
* *в результате;*
1. для дополнения и уточнения:
* *помимо этого, кроме того, также и, наряду с…, в частности;*
* *главным образом, особенно, именно;*
1. для иллюстрации сказанного:
* *например, так;*
* *проиллюстрируем сказанное следующим примером, приведем пример;*
* *подтверждением выше сказанного является;*
1. для ссылки на предыдущие высказывания, мнения, исследования и т.д.:
* *было установлено, рассмотрено, выявлено, проанализировано;*
* *как говорилось, отмечалось, подчеркивалось;*
* *аналогичный, подобный, идентичный анализ, результат;*
* *по мнению Х, как отмечает Х, согласно теории Х;*
1. для введения новой информации:
* *рассмотрим следующие случаи, дополнительные примеры;*
* *перейдем к рассмотрению, анализу, описанию;*
* *остановимся более детально на…;*
* *следующим вопросом является…;*
* *еще одним важнейшим аспектом изучаемой проблемы является…;*
1. для выражения логических связей между частями высказывания:
* *как показал анализ, как было сказано выше;*
* *на основании полученных данных;*
* *проведенное исследование позволяет сделать вывод;*
* *резюмируя сказанное;*
* *дальнейшие перспективы исследования связаны с….*

Письменная речь требует использования в тексте большого числа развернутых предложений, включающих придаточные предложения, причастные и деепричастные обороты. В связи с этим часто употребляются составные подчинительные союзы и клише:

* *поскольку, благодаря тому что, в соответствии с…;*
* *в связи, в результате;*
* *при условии, что, несмотря на…;*
* *наряду с…, в течение, в ходе, по мере.*

Необходимо определить основные понятия по теме исследования, чтобы использование их в тексте контрольной работы было однозначным. Это означает: то или иное понятие, которое разными учеными может трактоваться по-разному, должно во всем тексте данной работы от начала до конца иметь лишь одно, четко определенное автором курсовой работы значение.

В курсовом проекте должно быть соблюдено единство стиля изложения, обеспечена орфографическая, синтаксическая и стилистическая грамотность в соответствии с нормами современного русского языка.

# ПРИЛОЖЕНИЕ 1. Перечень тем курсового проектирования

1. Способы дистанционного управления СКУД.
2. Разработка системы видеоконтроля и системы контроля и управления доступа в страховой компании
3. Разработка системы контроля и управления доступа на стадионе.
4. Разработка системы контроля и управления доступа в метрополитене.
5. Разработка системы контроля и управления доступа в школе.
6. Модернизация системы контроля и управления доступом на предприятие Внедрение биометрической системы контроля доступа.
7. Методы биометрической идентификации.
8. Автономные и сетевые системы контроля и управления доступом.
9. Архитектура СКУД.
10. Биометрические системы контроля и управления.

# ПРИЛОЖЕНИЕ 2. Пример разработки введения контрольной работы

**ВВЕДЕНИЕ**

Тема моего контрольной работы является **актуальной**. Инженерно-техническая защита информации является одним из основных направлений обеспечения информационной безопасности. Технический прогресс способствует повышению роли инженерно-технической защиты. Она охватывает большое количество областей знаний и сфер практической деятельности органов внутренних дел, при ее обеспечении необходимо учитывать большое число факторов, информация о которых недостаточная и часто недостоверная.

Объекты информатизации органов внутренних дел предусматривают циркулирование конфиденциальной информации, как внутри подразделения, так и при обмене информацией с другими объектами информатизации органов внутренних дел. Актуально предусмотреть инженерно-техническую защиту вышеперечисленных объектов, первичным этапом которой является формирование проекта систем инженерно-технической защиты информации.

**Целью исследования моего контрольной работы** является совершенствование методики разработки проекта инженерно-технической защиты информации на объекте информатизации органов внутренних дел. **Задача контрольной работы** - рассмотрение решения следующих задач: анализа проекта инженерно-технической защиты информации, используемого на объекте информатизации органов внутренних дел; выявлением угроз безопасности информации, реализуемых в проекте систем инженерно-технической защиты информации; разработкой предложений по совершенствованию проекта систем инженерно-технической защиты информации объектов информатизации органов внутренних дел.

Выше изложенное в целом на теоретико-методологическом уровне определило **проблему настоящего исследования**: выявление достоинства и недостатков объекта информатизации органов внутренних дел и их использование в телекоммуникационных системах.

Недостаточная разработанность указанной проблемы и ее большая практическая значимость, определили тему исследования: «Методика разработки информации объектов информатизации органов внутренних дел».

**Гипотеза исследования -** рассмотрение основных объектов информатизации органов внутренних дел и выбор объекта с наилучшим показателями.

**Объект исследования** - является проект систем инженерно-технической защиты информации, используемый в объекте информатизации ОВД.

**Предмет исследования** - является методика разработки проекта инженерно-технической защиты информации, используемые в объектах информатизации органа внутренних дел.

**Методы исследования**: анализ многообразия технических средств для обеспечения безопасности информации, циркулирующей на объекте информатизации, синтез отдельных технических средств защиты информации в комплекс по защите информации, эксперимент, в целях построения модели функционирования проекта системы защиты информации эмпирическим путем.

В начале необходимо выделить способы реализации утечки информации и дать характеристику объекту информатизации с точки зрения защищаемой информации. На втором этапе разрабатывается предложения по защите информации и формируется алгоритм выбора оптимальных средств инженерно-технической защиты информации.

# ПРИЛОЖЕНИЕ 3. Пример оформления списка источников и литературы

**СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ**

**Нормативные материалы**

* + 1. ГОСТ Р 51275-99 от 01.01.99 4. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения
		2. ГОСТ Р.50922-2006. 5. Защита информации. Основные термины и определения.

**Научные, технические и учебно-методические издания**

3. Аверченков В.И., Рытов М.Ю., Кувыклин А.В., Гайнулин Т.Р Методы и средства инженерно-технической защиты информации. – БГТУ. - 2012.

4. Т.И. Булдакова, Б.В. Глазунов Математическое обоснование и теоретические аспекты информационной безопасности. УДК 004.056

5. Ворона В.А., Тихонов В.А. Инженерно-техническая и пожарная защита объектов. - Горячая линия - Телеком. – 2012.

6. В. К. Железняк Защита информации от утечки по техническим каналам, Учебное пособие, Санкт-Петербург, 2006

7. Каретников М.К. Технические каналы утечки информации. / Фондовая лекция по дисциплине «Инженерно- техническая защита информации». – М.: Московский университет МВД России. 2006.

8. Креопалов В.В. Технические средства и методы защиты информации. - Евразийский открытый институт. – 2011.

9. Петраков А.В. Основы практической защиты информации. М.: «Радио и связь», 1999 г.

10. Скрипник Д.А. Общие вопросы технической защиты информации. - Интернет-Университет Информационных Технологий (ИНТУИТ). – 2011.

11. Торокин А.А. Инженерно-техническая защита информации. / Учебное пособие. - М.: Гелиос АРВ, 2005.

12. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия РФ, 1998.

**Ресурсы сети Интернет**

http://infoacademy.ru/архив/учебник/раздел-1/глава-3.html

<http://avoidance.ru/articles/narushiteli-informacionnoj-bezopasnosti/77-metody-vyjavlenija-kanalov-utechki-rechevoj-informacii.html>.

[www.t-ss.ru](http://www.t-ss.ru)

# ПРИЛОЖЕНИЕ 4. Пример выполнения глав контрольной работы

**1 МЕТОДИКА АНАЛИЗА УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ**

**1.1 Определение характеристики объекта информатизации ОВД, с точки зрения защиты информации**

Важным этапом в методике разработки проекта систем инженерно-технической защиты информации на объекте информатизации органа внутренних дел является определение характеристик защищаемого объекта. Прежде чем принять какое-либо решение о необходимом уровне защиты, следует понять, что именно надо защищать и  в каких условиях. Часто этот важный шаг пропускают, и системы безопасности разрабатывают таким образом, что создают избыточную защиту несущественного имущества или не обеспечивают защиту важных частей объекта. Система, спроектированная с большим запасом надежности, может оказаться чрезмерно дорогой, а возможные последствия неадекватной защиты - разрушительными. Таким образом, очень важно, чтобы объект был полностью изучен с учетом налагаемых ограничений, рабочих процессов и условий деятельности.

При определении характеристик объекта должна быть собрана информация по возможно большему числу связанных с ним вопросов. Вначале это представляется очень сложной и многоплановой задачей, однако известно несколько аспектов, на которых следует сосредоточить внимание, чтобы получить нужную информацию. Они включают в себя:

1. Физические условия;
2. Специфика работы организации;
3. Должностные инструкции и подведомственные нормативно-правовые акты;
4. Требования органов государственного регулирования и вышестоящего руководства;
5. Вопросы аварийной безопасности.

**1. 2 Разработка модели угроз защищаемой информации**

Для обеспечения защиты информации необходимо знать, какие убытки можно понести в случае потери информации. Очевидно, что затраты на защиту не должны превышать возможных убытков при потере информации. Таким образом, необходимо ввести меру ценности информации, то есть определить, в каком смысле следует понимать ее ценность.

Сформулируем свойства информации, которые определяют ее ценность. Фундаментальными свойствами безопасности информации являются конфиденциальность, целостность, доступность.

Конфиденциальность определяется как свойство информации, которое состоит в том, что она не может быть доступной для ознакомления пользователям и/или процессам, не имеющим на это соответствующих полномочий.

Целостность информации – это свойство, которое состоит в том, что она не может быть доступной для модификации пользователям и/или процессам, не имеющим на это соответствующих полномочий. Целостность информации может быть физической и/или логической.

Доступность информации – это свойство, которое состоит в возможности ее использования по требованию пользователя, имеющего соответствующие полномочия.

Под угрозами понимаются пути реализации действий, которые считаются опасными. Например, угроза снятия информации и перехват излучения с дисплея ведет к потере конфиденциальности, угроза пожара ведет к нарушению целостности и доступности информации, угроза разрыва канала передачи информации может привести к потере доступности.

В общем случае модель угрозы защищаемой информации представлена на рисунке 1:

Способы реализации угрозы

Деструктивное действие

Объект воздействия

Уязвимость объекта

Рисунок 1 - Общая схема угрозы защищаемой информации

Потенциальными объектами атак нарушителя в объекте информатизации органа внутренних дел могут быть:

1.   Штатные аппаратные средства при использовании их санкционированными пользователями не по назначению и за пределами своих полномочий;

2.   Штатные аппаратные средства при использовании их посторонними лицами;

3.   Технологические пульты управления;

4.   Внутренний монтаж аппаратуры;

5.   Линии связи (коммуникаций) между аппаратными средствами АС;

6.   Побочные электромагнитные излучения и наводки аппаратных и телекоммуникационных средств обработки, и передачи информации АС, побочные наводки информации в сети электропитания и заземления аппаратуры АС, побочные наводки информации по цепям вспомогательных инженерных и других посторонних коммуникаций в отдельных помещениях и на территории АС;

7.   Отходы обработки информации в виде бумажных, магнитных и других носителей в мусорной корзине;

8.   Программное обеспечение;

9.   Другие возможные потенциальные каналы несанкционированного доступа и несанкционированного влияния.

Угрозы информации при разработке модели угроз удобно рассматривать с точки зрения их любого нежелательного действия и возможного нарушения свойств защищенности информации.

Таким образом, угроза – это потенциально возможное неблагоприятное воздействие на информацию, которое приводит к нарушениям хотя бы одного из приведенных свойств.

**1.3 Выявление каналов утечки информации**

Утечку информации в общем плане можно рассматривать как неправомерный выход конфиденциальных сведений за пределы организации или круга лиц, которым эти сведения были доверены.

По своей сущности утечка информации всегда предполагает противоправное (тайное или явное, осознанное или случайное) овладение конфиденциальной информацией, независимо от того, каким путем это достигается.

Виды каналов утечки информации (по виду опасного сигнала):

1. Оптические;
2. Акустические;
3. Электрические;
4. Электромагнитные.

Выявление каналов утечки информации возможно посредством:

1. Проверка помещений, объектов информатизации, информационных систем, автомобилей и технических средств специализированной аппаратурой.
2. Создание системы защиты информации.
3. Установка технических средств защиты информации.

Выявление способов утечки информации на объекте информатизации органа внутренних дел достигается посредством анализа потенциально возможных угроз информации, который в свою очередь является одним из первых и обязательных этапов разработки любой защищенной информационной системы. При этом составляется как можно более полная совокупность угроз, анализируется степень риска при реализации той или иной угрозы, после чего определяются направления защиты информации в конкретном объекте информатизации.

При определении угроз защищаемой информации на объекте информатизации следует определять не только масштаб возможных последствий при утечке информации, но и источники утечки информации.

Для каждого конкретного помещения объекта информатизации органа внутренних дел существует свой набор технических средств, которые могут создавать опасные сигналы и способствовать их распространению, т.е. служить источниками утечки.

Эти технические средства можно разделить на две основные группы:

1. Основные технические средства.
2. Вспомогательные технические средства и системы.

Каналы утечки информации можно классифицировать на функциональные и специальные.

Основное отличие этих двух категорий состоит в том, что функциональные каналы утечки информации объективно существуют на каждом объекте и их наличие вполне прогнозируемо. Специальные каналы утечки информации специально создаются вероятным противником с целью перехвата информации.

Для выявления как функциональных, так и специальных каналов утечки информации разработан и выпускается ряд технических средств. Данная аппаратура обобщенно называется - поисковой. Существует достаточно четкая классификация поисковой аппаратуры. Исходя из того, какие каналы можно выявить при помощи поисковых технических средств, их можно подразделить на две группы:

1. Аппаратура для выявление каналов утечки информации (работа по функциональным каналам).
2. Аппаратура для выявления и локализации технических средств перехвата информации (работа по специальным каналам).

Необходимость рассмотрения данного материала вызвана тем, что, как правило, руководство служб безопасности и технические специалисты групп поиска зачастую игнорируют вопросы выявления функциональных каналов утечки информации, всецело посвящая себя работе по специальным каналам. Иными словами, они уделяют основное внимание поиску подслушивающих устройств, в то время как в выделенных помещениях существуют более реальные угрозы - такие как шахты вентиляции, выходящие за зону контроля, щели в ограждающих конструкциях и т.д.

Опыт проведения поисковых мероприятий на различных объектах говорит о том, что практически в 90 % случаев в выделенных помещениях выявляются функциональные каналы утечки информации, в то время как специальные каналы существуют в 10 % случаев.

Из статистики видно, что почти в каждом выделенном помещении объекта информатизации существует потенциальная возможность перехвата информации. Этому есть объективное обоснование. Во-первых, задействовать функциональные каналы выгодно с экономической точки зрения, во вторых риск несомненно меньший, т.к. нет необходимости проникать на объект.

Таким образом, выявление функциональных каналов утечки информации выделенных помещений и последующая защита информации по этим каналам является залогом эффективности системы защиты информации на объекте.

**1.4 Выводы**

Подводя итог можно отметить, что методика анализа угроз безопасности информации на объектах информатизации органа внутренних дел состоит в определении характеристик объекта с точки зрения защищаемой информации, которое характеризуется такими аспектами, как физические условия; специфика работы организации; должностные инструкции и подведомственные нормативно-правовые акты; требования органов государственного регулирования и вышестоящего руководства; вопросы аварийной безопасности и так далее.

Так же методика анализа угроз безопасности информации состоит в разработке модели угроз защищаемой информации, которая представляет собой алгоритм действий нарушителя по отношению к потенциальным объектам его атак.

Важным аспектом методики анализа угроз безопасности информации является выявление каналов утечки информации, включающая в себя виды каналов утечки информации, методы выявления каналов утечки информации.

**2 ОПРЕДЕЛЕНИЕ СРЕДСТВ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫХ ДЛЯ ЗАЩИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ ОВД**

* 1. **Разработка предложений по защите информации на объекте информатизации ОВД**

В качестве примера объекта информатизации выступает кабинет начальника ОВД, так как в нем наиболее вероятно будет осуществляться циркулирование конфиденциальной информации.

На рисунке 2 представлен план кабинета начальника ОВД:







ШАБЛОН
МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ ДЛЯ СТУДЕНТОВ

ПО ВЫПОЛНЕНИЮ КОНТРОЛЬНОЙ РАБОТЫ





TV

Рисунок 2 - План кабинета начальника ОВД

В таблице 1 представлены условные обозначения к рисунку 2 – модели кабинета начальника ОВД:

*Таблица 1* Условные обозначения к рисунку 2

|  |  |  |
| --- | --- | --- |
| № п/п | Условное обозначение | Название объекта |
| 1 | BD18181_ | Стул |
| 2 | TV | Телевизор |
| 3 |  | Дверь |
| 4 | BD18225_ | Телефонный аппарат |
| 5 | BD18221_ | Персональный компьютер |
| 6 |  | Отверстие вентиляции |
| 7 |  | Платяной шкаф |
| 8 |  | Розетка |
| 9 |  | Сейф |
| 10 |  | Окно |
| 11 |  | Радиатор центрального отопления |
| 12 | BD18182_ | Рабочее кресло |
| 13 |  | Цепь электропитания |

В таблице 2 представлены технические характеристики кабинета начальника ОВД:

*Таблица 2* Характеристики кабинета начальника ОВД

| № п/п | Наименование характеристики | Значение |
| --- | --- | --- |
| 1 | Назначение помещения | Кабинет начальника ОВД |
| 2 | Режим посещения | Начальник ОВД, сотрудники в присутствии начальника ОВД. |
| 3 | Площадь | 50 м2 |
| 4 | Капитальные стены | Железобетонная панель, толщина - 300 мм |
| 5 | Окна (число, характер рам, стекла) | 2 пластиковых окна, 2 форточки, рамы пластиковые |
| 6 | Двери | Дверное полотно, размер 200х120 мм, выполненное из цельного дерева. |
| 7 | Смежные помещения, их назначение, материал стен, толщина. | Слева – кабинет начальника полиции ОВД, справа – кабинет юрисконсульта, материал стен – железобетонные панели, толщина 300 мм. |
| 8 | Смежные помещения вверху, их назначение, материал перекрытия, толщина | Кабинет начальника тылового обеспечения, железобетонная панель, толщина – 300 мм |
| 9 | Смежные помещения внизу, их назначение, материал перекрытия, толщина | Дежурная часть ОВД, железобетонная панель, толщина – 300 мм |
| 10 | Вентиляционные отверстия, их размер | 1 отверстие, 220х160 мм |
| 11 | Инженерные системы (отопления, канализация, водоснабжение) | 2 радиатора центрального отопления с вертикальными подводными трубами |
| 12 | Звукопоглощающие конструкции, место их установки, материал изготовления | Подвесной потолок, материал – акустические плиты «Акмигран» 500х500 мм, глубина межпотолочного пространства – 300 мм |
| 13 | Цепи электропитания, число розеток, напряжение | 220 В, 50 Гц, 6 розеток |
| 14 | Телефон, тип аппарата, место установки, тип кабеля | 2 абонентских телефонных линии городской АТС: 1- PANASONIC KX-TS2350RUB, 2 - PANASONIC KX-TС1703, беспроводной, с режимом «громкая связь»; 1 выделенная телефонная линия для связи с УВД - PANASONIC KX-TS2350RUB, тип кабеля: ТРП-2 |
| 15 | Персональный компьютер, место установки, наличие локальной сети | 1 персональный компьютер, станция локальной сети ОВД |
| 16 | Бытовые электроприборы | Телевизор LG 2LA643V c функцией видеопроигрывателя  |
| 17 | Технические средства охранно-пожарной сигнализации | 3 потолочных датчика пожара – ИП-212-9 |
| 18 | Предметы интерьера | Рабочее кресло, сейф, 2 платяных шкафа, 10 стульев, письменный стол |

В целях защиты кабинета от утечки информации актуальны следующие предложения: так как проникновение злоумышленника возможно через дверь в кабинет, необходимо создать защитный рубеж. Для этого на дверь из коридора в кабинет устанавливается магнитоконтактный извещатель типа СМК-3, стоимостью 200 рублей, или более современные ИО-104-4, стоимостью 600 рублей. Датчик ИО-104-4 имеет меньшие габариты. Эти извещатели обеспечивают замыкание и размыкание контактов геркона при приближении магнита к геркону на расстояние не более 10 мм контакты и удалении более 45 мм. В кабинете начальника ОВД устанавливаем ИО-104-4

В кабинете можно установить пассивный оптикоэлектронный, ультразвуковой, радиоволновый и комбинированный извещатели. Выбор производится по таким характеристикам, как помехоустойчивость, объёму кабинета и затрат на приобретение и эксплуатацию. Средства охраны кабинета при отсутствии на рабочем месте руководителя организации целесообразно сохранять во включённом состоянии. Для обеспечения такого режима необходимо использовать блоки бесперебойного питания.

Учитывая небольшую площадь кабинета, целесообразно применять или пассивные оптико-электронные извещатели или активные волновые с регулируемой мощностью излучения. В качестве таких средств могут использоваться оптико-электронный извещатель «Фотон-5», стоимостью 500 рублей, ультразвуковой «Эхо-2», стоимостью 400 рублей, радиоволновой объёмный «Волна-5», стоимостью 2000 рублей, и комбинированный извещатель «Сокол-2», стоимостью 1500 рублей, совмещающий пассивный инфракрасный и радиоволновой принципы обнаружения. Последний обеспечивает дальность действия: минимальную – 3-5 м, максимальную – 12 м. Он может крепиться к стене или на потолке, имеет высокую помехоустойчивость. Из сравнительного анализа указанных извещателей можно сделать вывод о том, что наиболее дешёвым извещателем с приблизительно равными функциональными возможностями является оптико-электронный извещатель «Фотон-5». По критерию эффективность/стоимость лучшие показатели имеет комбинированный извещатель «Сокол-2».

Кроме рассмотренных средств целесообразно установить локальные извещатели для охраны компьютера. Для защиты информации в компьютере от физического контакта его со злоумышленником и хищения информации путём копирования или изъятия винчестера в качестве извещателя можно использовать ёмкостной извещатель «Пик», стоимостью 1000 рублей, или извещатель «АЛАРТ», последний имеет большую стоимость, при одинаковой эффективности. Для механической защиты системный блок с винчестером может быть размещён в специальном сейфе под приставным столиком или использоваться съёмный винчестер, помещаемый в сейф. Используем извещатель «Пик» в кабинете начальника ОВД.

Для защиты информации от наблюдения применяются методы энергетического скрытия путём увеличения затухания среды распространения. Для прекращения функционирования оптического канала утечки информации «окно кабинета – окно противоположного жилого дома» можно применить следующие меры:

1. Шторы на окна;
2. Жалюзи;
3. Тонированные плёнки на стёклах.

В кабинете начальника ОВД используем жалюзи, стоимостью 2000 рублей.

Для защиты от утечки речевой информации в кабинете необходимо существенно повысить звукоизоляцию дверей как наиболее слабого звена в акустической защите и стены по крайней мере, до 55 дБ на частоте 1000 Гц. Такая звукоизоляция обеспечивается двойной дверью с тамбуром шириной не менее 20 см с уплотнителями по периметру дверных полотен.

В качестве меры, повышающей энергетическое скрытие речевой информации в кабинете, на стенах могут быть укреплены виброакустические излучатели акустического генератора помех «Барон». Наиболее актуально установить этот прибор в кабинете начальника ОВД, так как он более эффективный и менее громоздкий, хоть и с большей стоимостью 10000 рублей.

Для исключения утечки информации через батареи и трубы отопления перед батареями устанавливают резонансные экраны в виде деревянных перегородок с отверстиями, или используются виброакустические преобразователи прибора «Барон». В соотношении эффективности и цены наиболее рационально использовать средство «Барон».

Для предотвращения утечки информации через вентиляционное отверстие, пред ним укрепляют экран и (или) размещают в нём глушитель звука, выполненный из пористого материала.

Для исключения возможности функционирования скрыто установленного диктофона применяем средство «Бубен», стоимостью 12000 рублей, или «Хамелеон XL», стоимостью 23000, последний имеет наибольшую площадь зашумления, выходящую за пределы кабинета начальника ОВД, в результате чего оснащаем кабинет средством «Бубен».

В целях подавления сотовых сигналов во время конфиденциальных совещаний в кабинете необходимо предусмотреть генератор шума «[Аллигатор 100+4G LTE»,](http://www.gf-domof.ru/product/?id=342) с помощью которого возможно подавить сигнал 3G и 4G сети, стоимостью 14000 рублей, или ПБ-4G, стоимостью 18000 рублей, последний прибор охватывает наибольшую площадь, и имеет наибольшую стоимость, в кабинете начальника ОВД используем прибор «[Аллигатор 100+4G LTE»](http://www.gf-domof.ru/product/?id=342).

Необходимо установить средство подавления сигналов акустоэлектрических преобразователей телефонных аппаратов типа «Корунд», стоимостью 1400 рублей или «Гранит-VIII» - ограничителей малых амплитуд с фильтрами от ВЧ-навязывания, стоимостью 2000 со сравнительно одинаковыми характеристиками. С экономической точки зрения оснащаем кабинет начальника средством «Корунд».

Путем сложения цен выбранных устройств получаем сумму 46 500 рублей.

С учётом рассмотренного в качестве мер предотвращения подслушивания рекомендуется:

1. Установка виброакустических генераторов шума изделия «Барон» на окна, двери и батареи.
2. Закрытие окон с помощью жалюзи, установка на стёкла окон излучателей генератора виброакустического зашумления (для предотвращения лазерного подслушивания при закрытых окнах изделия «Барон»).
3. Установка перед воздухозаборниками воздухопроводов акустических экранов, выполненных из пористого материала.
4. Применение устройств для подавления сигналов скрытно работающего диктофона изделием «Бубен».

Предотвращение утечки информации из кабинета по радиоэлектронному каналу обеспечивается:

1. Выключением во время разговора всех радиосредств и электрических приборов, без которых можно обойтись.
2. Установкой в разрыв цепей электропитания возле стен сетевых фильтров для исключения ВЧ-навязывания.
3. Установкой средств подавления сигналов акустоэлектрических преобразователей телефонных аппаратов типа «Корунд» или «Гранит-VIII» - ограничителей малых амплитуд с фильтрами от ВЧ-навязывания.
4. Установить генератор шума «[Аллигатор 100+4G LTE»,](http://www.gf-domof.ru/product/?id=342) в целях подавления сотовых сигналов.

На рисунке 3 представлен кабинет начальника ОВД, оснащенный вышеперечисленными средствами инженерно-технической защиты информации:



Рисунок 3 - План кабинета начальника ОВД, оснащенная средствами ИТЗИ

В таблице 3 представлены условные обозначения к рисунку 3 – план кабинета начальника ОВД, оснащенная средствами ИТЗИ:

*Таблица 3* Условные обозначения к рисунку 3

| № п/п | Условное обозначение | Название объекта |
| --- | --- | --- |
| 1 | Сокол-2 | Комбинированный извещатель «Сокол-2» |
| 2 | Барон | Акустический генератор помех «Барон» |
| 3 |  | Магниито-контактный извещатель ИО-104-4 |
| 4 | Аллигатор | Генератор шума «[Аллигатор 100+4G LTE»](http://www.gf-domof.ru/product/?id=342) |
| 5 | корунд | Подавитель сигналов акустоэлектрических преобразователей телефонных аппаратов «Корунд» |
| 6 | сф | Сетевой фильтр |
| 7 |  | Жалюзи |
| 8 | Пик | Емкостный извещатель «Пик» |

Стоит обратить внимание и на организационные меры по защите информации. К ним относятся:

1. Организацию охраны помещений и разработку пропускного режима;
2. Ограничение доступа в помещения, где размещены серверы автоматизированной системы управления;
3. Хранение носителей информации и бумажной документации в сейфах или других защищенных местах;
4. Установку мониторов компьютеров, клавиатуры, принтеров таким образом, чтобы исключить возможность просмотра или копирования информации посторонними лицами;
5. Ликвидацию ненужных носителей информации и документов;
6. Уничтожение всей информации на жестких дисках компьютеров, где были установлены компоненты системы, перед их отправкой в ремонт;
7. Проведение регулярных проверок по соблюдению всех правил, положений и инструкций, связанных с обеспечением информационной безопасности.
	1. **Алгоритм выбора оптимальных средств инженерно-технической защиты информации**

В первую очередь стоит отметить, что все средства инженерно-технической защиты информации должны быть сертифицированы ФСТЭК и ФСБ России.

Выбор средств инженерно-технической защиты информации осуществляется на этапе реализации мер защиты кабинета с учетом уровня защищенности и наличия актуальных угроз безопасности информации. В общем виде порядок выбора СЗИ можно представить в виде схемы, представленной на рисунке 4:



Рисунок 4 - Порядок выбора средств инженерно-технической защиты информации

При выборе средств инженерно-технической защиты информации необходимо провести анализ угроз защищаемой информации, дать экономическую оценку защищаемой информации, в случае её разглашения и на основе полученных результатов принять решение о оснащении служебного помещения конкретными средствами инженерно-технической защиты информации.

Следует перечислить рекомендации по выбору оптимальных средств защиты информации кабинета начальника ОВД:

1. Затраты на средства инженерно-технической защиты информации должны быть экономически обоснованы.
2. Средства защиты информации должны функционировать только на заданной территории.
3. Анализировать возможности средств негласного получения информации, используемых нарушителем и на основе анализа осуществлять подбор средств защиты.
4. Определить степень взаимодействия средств защиты между собой.
5. Определяется степень участия персонала, функциональных служб, специалистов и вспомогательных работников объекта автоматизации в обработке информации, характер их взаимодействия между собой и со службой безопасности.
6. Средства инженерно-технической защиты информации должны функционировать непрерывно.

**2.3 Выводы**

Во втором разделе были предложены следующие мероприятия, позволяющие эффективно защитить исследуемый кабинет:

1. Применение пассивных оптико-электронных извещателей или активных волновых с регулируемой мощностью излучения (например, оптико-электронный извещатель «Фотон-5», ультразвуковой «Эхо-2», радиоволновой объёмный «Волна-5», комбинированный извещатель «Сокол-2»).
2. Использование для защиты информации в компьютере от физического контакта его с противником и хищения информации путём копирования или изъятия винчестера ёмкостного извещателя «Пик».
3. В целях прекращения функционирования оптического канала утечки информации «окно кабинета – окно противоположного жилого дома» можно применить следующие меры: шторы на окна, жалюзи, тонированные плёнки на стёклах;
4. В целях предотвращения утечки информации через ограждения кабинета возможно проведение следующих мероприятий, направленных на: повышение поверхностной плотности ограждения, установление дополнительной перегородки, зашумление ограждения.
5. Предотвращение утечки информации из кабинета по радиоэлектронному каналу обеспечивается: выключением во время разговора всех радиосредств и электрических приборов, без которых можно обойтись, установкой в разрыв цепей электропитания возле стен сетевых фильтров для исключения ВЧ-навязывания, установкой средств подавления сигналов акустоэлектрических преобразователей телефонных аппаратов типа «Корунд» и «Гранит-VIII» - ограничителей малых амплитуд с фильтрами от ВЧ-навязывания.

Так же были предложены рекомендации и алгоритм выбора средств инженерно-технической защиты информации.

**ЗАКЛЮЧЕНИЕ**

В курсовом проекте представлена методика совершенствования проекта инженерно-технической защиты информации на примере кабинета начальника ОВД

В первой главе представлена методика анализа угроз безопасности информации на объектах информатизации органа внутренних дел состоит в определении характеристик объекта с точки зрения защищаемой информации, которое характеризуется такими аспектами, как физические условия; специфика работы организации; должностные инструкции и подведомственные нормативно-правовые акты; требования органов государственного регулирования и вышестоящего руководства; вопросы аварийной безопасности и так далее.

Так же методика анализа угроз безопасности информации состоит в разработке модели угроз защищаемой информации, которая представляет собой алгоритм действий нарушителя по отношению к потенциальным объектам его атак.

Важным аспектом методики анализа угроз безопасности информации является выявление каналов утечки информации, включающая в себя виды каналов утечки информации, методы выявления каналов утечки информации.

Во второй главе были предложены следующие мероприятия, позволяющие эффективно защитить исследуемый кабинет:

1. Применение пассивных оптико-электронных извещателей или активных волновых с регулируемой мощностью излучения (например, оптико-электронный извещатель «Фотон-5», ультразвуковой «Эхо-2», радиоволновой объёмный «Волна-5», комбинированный извещатель «Сокол-2»).
2. Использование для защиты информации в компьютере от физического контакта его с противником и хищения информации путём копирования или изъятия винчестера ёмкостного извещателя «Пик».
3. Использование для защиты акустического канала утечки информации кабинета начальника ОВД используем генератор акустического «Шума».
4. В целях прекращения функционирования оптического канала утечки информации «окно кабинета – окно противоположного жилого дома» можно применить следующие меры: шторы на окна, жалюзи, тонированные плёнки на стёклах.
5. В целях предотвращения утечки информации через ограждения кабинета возможно проведение следующих мероприятий, направленных на: повышение поверхностной плотности ограждения, установление дополнительной перегородки, зашумление ограждения.
6. Предотвращение утечки информации из кабинета по радиоэлектронному каналу обеспечивается: выключением во время разговора всех радиосредств и электрических приборов, без которых можно обойтись, установкой в разрыв цепей электропитания возле стен сетевых фильтров для исключения ВЧ-навязывания, установкой средств подавления сигналов акустоэлектрических преобразователей телефонных аппаратов типа «Корунд» и «Гранит-VIII» - ограничителей малых амплитуд с фильтрами от ВЧ-навязывания.

Выбор вышеперечисленных приборов экономически обоснован. Так же были предложены рекомендации и алгоритм выбора средств инженерно-технической защиты информации. Таким образом можно сделать вывод о том, что задачи выполнены, цель курсовой работы достигнута.