

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВО «Севастопольский государственный университет»
Институт радиоэлектроники и информационной безопасности
Кафедра информационной безопасности

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Задания и методические рекомендации к
выполнению курсового проекта**

для студентов очной и очно-заочной форм обучения
специальности 10.03.01 «Информационная безопасность»

Севастополь
2015

УДК 004.056.53

Основы информационной безопасности : задания и методические рекомендации к выполнению курсового проекта для студентов очной и очно-заочной форм обучения специальности 10.03.01 «Информационная безопасность» / СевГУ; сост. В. М. Шахайда, А. О. Калита. — Севастополь: изд-во ФГАОУ ВО «СевГУ», 2015. — 76 с.

В методических рекомендациях изложены общие требования к разработке, построению, изложению и оформлению курсового проекта по изучению технических каналов утечки информации, которые могут быть реализованы на объектах информатизации.

Методические рекомендации утверждены на заседании кафедры информационной безопасности института радиоэлектроники и информационной безопасности «28» августа 2015 года, протокол № 1.

Рецензент: профессор, доктор технических наук,
профессор кафедры радиоэлектроники и
телекоммуникаций института радиоэлектроники и
информационной безопасности
Афонин И. Л.

Содержание

Введение	5
Термины и определения	6
1. Основные требования к курсовому проекту	10
1.1. Цель и задачи курсового проекта.....	10
1.2. Выбор темы курсового проекта.....	10
1.3. Составление индивидуального календарного плана.	11
2. Требования к пояснительной записке и оформлению чертежей.....	14
2.1. Общие требования по структуре пояснительной записки	14
2.2. Введение	14
2.3. Основные разделы пояснительной записки	16
2.4. Заключение.....	16
2.5. Приложения.....	18
2.6. Библиографический список	18
2.7. Стилистические рекомендации	19
2.8. Оформление текстового материала	21
2.9. Подготовка к защите курсового проекта.....	33
Приложение А. Образец оформления титульного листа	34
Приложение Б. Образец задания на курсовой проект	35
Приложение В. Образец выполнения курсового проекта...	38
Приложение Г. Ситуационный план	62
Приложение Д. Генеральный план.....	63
Приложение Е. Акустический канал утечки информации .	64
Приложение Ж. Проект комнаты в 3d формате	65
Приложение И. Ранжирование источников угроз	66

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АС	—	автоматизированная система;
АТС	—	автоматическая телефонная станция;
ВТСС	—	вспомогательные технические средства и системы;
ВЧ	—	высокая частота;
ИсОД	—	информация с ограниченным доступом;
КЗ	—	контролируемая зона;
ЛСАР	—	лазерное средство акустической разведки;
ЛЭП	—	линии электропитания;
МНД	—	микрофон направленного действия;
МУ	—	модель угроз для информации;
МФУ	—	многофункциональных устройств;
НСД	—	несанкционированный доступ;
ОИ	—	объект информатизации;
ОТС	—	основные технические средства;
ПЭМИН	—	побочные электромагнитные излучения и наводки;
СТР	—	средство технической разведки;
ТЗИ	—	техническая защита информации;
ТКУИ	—	технический канал утечки информации;
ТР	—	техническая разведка;
ТС	—	технические средства;
ТСОИ	—	технические средства обработки информации.

ВВЕДЕНИЕ

Область знаний по предмету «Основы информационной безопасности» охватывает несколько дисциплин подготовки студентов по направлению «Информационная безопасность». К ним относятся вопросы: нормативно-правового обеспечения, физических основ каналов утечки информации, правил обращения с документами конфиденциального характера. Наиболее сложным в понимании студентов является анализ оперативной ситуации на объекте информатизации и прилегающей к нему территории. Информация, изложенная в методическом пособии, позволяет систематизировать знания полученные в ходе изучения дисциплины «Основы информационной безопасности». В пособии даны практические рекомендации по подготовке к написанию курсового проекта, сбору информации, порядку изложения информации. Приведен пример описания генерального и ситуационного плана. Рассмотрен пример описания технических каналов утечки информации и методы оценки их опасности.

Изложены правила оформления работы в соответствии с требованиями ГОСТ и нормативными актами.

Пособие предназначено для студентов, обучающихся по направлению 10.03.01 «Информационная безопасность» может быть полезна для студентов других специальностей.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины и определения приводятся в соответствии с ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

Анализ риска — систематическое использование информации для определения источников риска и количественной оценки риска.

Атака «отказ в обслуживании» — сетевая атака, приводящая к блокированию информационных процессов в автоматизированной системе.

Блокирование доступа (к информации) — прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей).

Вспомогательные технические средства и системы — непосредственно непредназначенные для обработки информации с ограниченным доступом технические средства и системы на объекте информатизации, которые могут создавать каналы ее утечки под влиянием на них электрических, магнитных полей основных технических средств или акустических сигналов.

Защищаемый процесс (информационной технологии) — процесс, используемый в информационной технологии для обработки защищаемой информации с требуемым уровнем ее защищенности.

Идентификация риска — процесс обнаружения, распознавания и описания рисков.

Инцидент информационной безопасности — любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Источник риска информационной безопасности организации — объект или действие, способное вызвать [создать] риск.

Информационная безопасность организации — состояние защищенности интересов организации в условиях угроз в информационной сфере.

Информативный сигнал — сигнал, по параметрам которого может быть определена защищаемая информация.

Модель угроз (безопасности информации) — физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Нарушитель информационной безопасности организации — физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации.

Нарушение информационной безопасности организации — случайное или преднамеренное неправомерное действие физического лица (субъекта, объекта) в отношении активов организации, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах, вызывающее негативные последствия (ущерб/вред) для организации.

Недекларированные возможности — функциональные возможности средств вычислительной техники и программного обеспечения, не описанные или не соответствующие описанным в документации, которые могут привести к снижению или нарушению свойств безопасности информации.

Несанкционированный доступ — доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа.

Объект защиты информации — информация или носитель информации, или информационный процесс, которую(ый) необходимо защищать в соответствии с целью защиты информации.

Обработка риска информационной безопасности организации — процесс разработки и/или отбора и внедрения

мер управления рисками информационной безопасности организации.

Основные технические средства — технические средства на объекте информатизации, которые непосредственно предназначены для обработки информации с ограниченным доступом: средства вычислительной техники, связи, аудио-, видео-, копировально-множительной техники (электрофотографические, светло-, микро-, фото-, термокопировальные и другие), средства изготовления графических и текстовых документов (электромеханические, электронные печатные машинки), телеграфные и факсимильные аппараты, другие средства обработки информации.

Опасная ситуация — обстоятельства, в которых люди, имущество или окружающая среда подвергаются опасности.

Определение приемлемости уровня риска — процесс сравнения результатов анализа риска с критериями риска с целью определения приемлемости или допустимости уровня риска.

Оценка риска — процесс, объединяющий идентификацию риска, анализ риска и их количественную оценку.

Перехват (информации) — неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Побочные электромагнитные излучения и наводки — электромагнитные излучения технических средств обработки информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Разглашение информации — несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации.

Риск — влияние неопределенностей на процесс достижения поставленных целей.

Событие — возникновение или наличие определенной совокупности обстоятельств.

Угроза информационной безопасности организации — совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации.

Угроза (безопасности информации) — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Управление рисками — координированные действия по направлению и контролю над деятельностью организации в связи с рисками.

Утечка информации — неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками.

Уязвимость (информационной системы) — свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

1. ОСНОВНЫЕ ТРЕБОВАНИЯ К КУРСОВОМУ ПРОЕКТУ

1.1. Цель и задачи курсового проекта

Курсовой проект по дисциплине «Основы информационной безопасности» выполняется на 5 семестре обучения и является логическим итогом изучения блока вопросов, касающихся изучения возможных каналов утечки информации на объектах информатизации.

Целью курсового проекта является систематизация, закрепление тематических и практических знаний по специальности и применение их при решении конкретных инженерных задач.

Достижение цели обеспечивается последовательным выполнением следующих этапов: выбор темы курсового проекта, составление индивидуального календарного плана работы, оформление пояснительной записки и чертежей (плакатов), подготовка к защите работы.

Руководителями курсовых проектов назначаются, как правило, ведущие преподаватели кафедры информационной безопасности или другие профессора и доценты института радиоэлектроники и информационной безопасности. Кандидатуры руководителей и темы курсовых проектов обсуждаются на заседании кафедры информационной безопасности института радиоэлектроники и информационной безопасности, после чего утверждаются приказом заведующего кафедрой.

1.2. Выбор темы курсового проекта

В процессе выполнения курсового проекта студент должен проявить знания в следующих областях:

- основам информационной безопасности;
- пакетов стандартных и прикладных программных продуктов;

- теории вероятностей и математических методов оптимизации и исследование операций;
- создании баз данных и знаний и системном анализе;
- компьютерной графике и информатике;
- проектировании компьютерных информационных систем.

В процессе обучения в институте и, особенно, на стадии выполнения курсового проекта студент должен выработать необходимые навыки работы в области защиты информации. Проект выполняется на основе теоретических знаний студента и его практических навыков, полученных в результате обучения.

Главное требование к курсовому проекту состоит в том, что он должен решать конкретную инженерно-техническую задачу путём создания модели угроз для реального объекта информатизации. Это позволяет самостоятельно произвести анализ исходных материалов, обобщить их, сформулировать задачу и определить порядок её решения.

1.3. Составление индивидуального календарного плана

К курсовому проекту допускаются студенты, полностью завершившие курс обучения в соответствии с учебным планом.

После утверждения темы и руководителя курсового проекта приказом директора института радиоэлектроники и информационной безопасности, студент с помощью руководителя должен организовать свою работу так, чтобы выполнить её с наименьшей затратой времени и максимальным качеством. Для этого необходим календарный план курсового проектирования, который связывает воедино все этапы работы над курсовым проектом и строго регламентирует их по времени.

Как правило, календарный план выполнения курсового проект включает следующие основные этапы:

— уяснение задачи в соответствии с темой курсового проекта.

- решение поставленной задачи.
- анализ результатов внедрения работы.
- написание пояснительной записки.
- рецензирование работы.
- оформление чертежей (плакатов).
- подготовка к защите проекта.

С самого начала работы студент должен четко уяснить задачу, поставленную перед ним, то есть должен знать, что именно и в каком объеме он должен выполнить разделы курсового проекта. Безусловно, чтобы понять поставленную перед студентом задачу, он должен, достаточно свободно ориентироваться в этой области и иметь необходимый минимум материала и знаний ума её решений.

Решение поставленной задачи должно носить творческий, новаторский подход и не сводится только к техническим вопросам. Курсовой проект оценивается по степени и глубине всех заданий, предусмотренных темой, а именно: теоретических, технических и эксплуатационных. Решая задачу, необходимо стремиться не повторять уже имеющиеся решения, а искать новые, оригинальные подходы. Курсовой проект — это результата самостоятельной творческой работы студента. Тем не менее, здесь целесообразно напомнить о существующих типовых этапах решения поставленной задачи.

Во-первых, это **анализ материала**. Как правило, это обзор учебно-методических пособий, современных научных публикаций, возможностей интернет ресурсов и др., посвященных области знаний, в которой предстоит решать конкретную инженерную задачу. При обработке этого материала необходимо отмечать, каким образом рассматриваемые в источниках ситуации соответствуют поставленной задаче, насколько эффективны решения, можно ли их применять в других условиях. Это, самая ответственная и продолжительная по временным затратам работа.

Во-вторых, **определение условий** решения задачи. Главным образом это изучение конкретного объекта или процесса, который предстоит моделировать или алгоритмизировать. Определение его пространственно-временных характеристик, то есть определение конкретных геометрических границ и продолжительность по времени в течении которого этот процесс происходит. После этого строго выяснить где, что и при каких условиях будет решаться задача, какими будут входные (исходные) данные и что мы получим на выходе. Значение имеет также и определение круга лиц, в отношении которых будет производиться разработка модели угроз. То есть необходимо решить от кого мы будем защищаться (уровень профессионализма злоумышленника, его материальные и технические возможности).

В-третьих, **само решение** задач. Оно может быть в различном виде (математической формулы, управляющего алгоритма, экспертного решения и т.д.).

В-четвертых, **описание алгоритма**, обеспечивающего инженерное решение поставленной задачи.

Анализ результатов внедрения (или возможного внедрения) рассматриваемой инженерной задачи осуществляется в трех аспектах.

Написание пояснительной записки оформление чертежей и подготовка выступления по работе производится в строгом соответствии с данными методическими рекомендациями.

2. ТРЕБОВАНИЯ К ПОЯСНИТЕЛЬНОЙ ЗАПИСКЕ И ОФОРМЛЕНИЮ ЧЕРТЕЖЕЙ

2.1. Общие требования по структуре пояснительной записки

Пояснительная записка по своему содержанию должна соответствовать теме курсового проекта и в краткой, сжатой форме раскрывать результаты проведенного исследования ИОД, его реализацию, расчеты их описание, анализ и выводы, которые при необходимости сопровождаются иллюстрациями, графиками, эскизами, диаграммами, схемами и т.д.

Типовая структура пояснительной записки содержит:

- титульный лист;
- задание на курсовой проект;
- содержание;
- перечень сокращений, специальных символов и терминов;
- введение;
- основные разделы курсового проекта;
- заключение.

2.2. Введение

Введение к курсовому проекту должно включать в обязательном порядке следующие подразделы.

Актуальность темы. Кратко обосновывается актуальность темы, какими причинами она вызвана и обусловлена в конкретной области науки, техники, производства и т.д.

Цель и задачи работы. Здесь формируется конкретная цель, которая стоит перед студентом, например: «Изучение каналов утечки информации для объекта информатизации расположенного в помещении № 423».

Далее раскрывается, что конкретно необходимо выполнить при проектировании, какие задачи решить для достижения заданной цели, то есть

- проанализировать ..., разработать ...,
- рассмотреть ..., экспериментально проверить ... и

т.д.

Теоретическое и практическое значение работы.

Дается оценка работы с точки зрения теории и практики конкретной отрасли деятельности, в которой решается инженерная задача. Показывается объем фактических материалов, положенных в основу работы их достаточность для формулировки выводов.

Область внедрения. Где конкретно данное инженерное решение применяется или может быть внедрено, а также, условия, необходимые для этого внедрения.

Структура работы. Перечисляется что работа состоит из введения, трех или более разделов, заключения, литературы из... (такого числа) источников, приложение (одного, двух..., если они есть, описи графического материала, содержит... листов машинописного или рукописного текста, ... рисунков, ... таблиц).

Необходимо подчеркнуть, что для абсолютного большинства студентов эта работа является первым самостоятельным трудом и, не имея опыта оформительской работы текстовых документов, многие из них зачастую делают ошибку, когда начинают писать пояснительную записку с введения. В таком случае на его составление затрачивается немало времени, а при завершении работы нередко оказывается, что оно по содержанию не соответствует своему назначению.

Заканчивать введение следует изложением целевой установки работы.

2.3. Основные разделы пояснительной записки

В разделах пояснительной записки, отражающих методику, содержание и результаты выполненных исследований, подробно и последовательно излагается содержание работы, и описываются все промежуточные и окончательные результаты, в том числе результаты отрицательные.

Методика исследования должна излагаться подробно, с обоснованием её выбора. Если в курсовом проекте применяются общепринятые методы, их описание подробно не приводится, а даются ссылки на источники, которые нумеруются в хронологическом порядке и заключаются в квадратные скобки.

В разделе, посвященном описанию исследований, указывается цель и описывается программа конкретных исследований, излагается их сущность, описывается точность и достоверность полученных результатов и сопоставляются с теоретическими данными.

Эти разделы пояснительной записки завершаются трактовкой полученных результатов и описанием их возможного применения.

Пояснительная записка должна включать в себя обоснование принятых методов расчета и сам расчет, а также наиболее существенные стороны проекта, представляющие теоретический и практический интерес. Результаты расчетов рекомендуется сводить в таблицы, конечные результаты должны быть отображены в тексте записки.

2.4. Заключение

В конце каждого раздела пояснительной записки, особенно разделов, раскрывающих основное содержание курсовой работы, необходимо делать краткие выводы по рассмотренным в них вопросам.

В выводах словами выделяется то наиболее существенное, что явилось предметом исследования, показываются новые элементы, выявленные, подмеченные или открытые студентом — проектантом с позиции его темы, благодаря его работе.

Из выводов данного раздела определенным образом должна вытекать целесообразность и необходимость рассмотрения круга проблем или вопросов, которым посвящаются последующие главы. В этом отношении выводы разделов должны служить связующим звеном между отдельными частями курсового проекта.

В заключении следует изложить в развернутом виде обобщение наиболее существенных положений и итогов всей проделанной в процессе работы по данной теме и указать на нерешенные вопросы, которые потребуют дальнейшей разработки. Последнее очень важно и для выпускника, и для кафедры.

Заключение не должно быть простым перечислением принятых в работу решений или изложением её содержания.

В заключении намечаются пути и цели дальнейшей работы, дается оценка технико-экономической эффективности, которая может быть получена при использовании результатов выполненной работы.

Заключение по курсовому проекту в целом дается в виде трех четырех основных положений. В ней кратко перечисляют то, что установлено в процессе работы, последовательно излагаются полученные автором результаты.

По форме изложения заключение должно напоминать характер тезисов, то есть в конце заключения указываются основные результаты, которые достигнуты в итоге выполнения работы (то есть выводы по курсовой работе): составлены инструкции, правила, наставления, методики расчетов, измерений, испытаний; разработаны нормы и правила, алгоритмы, программы и т.д.

2.5. Приложения

В приложение следует включать вспомогательный, но необходимый по ходу изложения курсового проекта, материал, который в основную часть пояснительной записки включать нецелесообразно, так как он загромождает текст.

К вспомогательному материалу относятся:

- промежуточные математические вкладки и расчеты;
- таблицы вспомогательных цифровых данных;
- протоколы и акты испытаний;
- описания аппаратуры и приборов, примененных при проведении экспериментов, измерений и испытаний;
- инструкции, методики и т.п., разработанные в процессе выполнения проекта.

Приложения располагаются в порядке появления ссылок в тексте основных разделов. Если приложений больше 10, то их объединяют по видам: промежуточные математические выкладки и расчеты, результаты испытаний и т.д.

2.6. Библиографический список

Библиографический список приводится в конце пояснительной записки. В него включаются все источники, которые были использованы при выполнении работы.

Источники располагают в порядке появления ссылок в тексте. Сведения о книгах должны включать фамилию инициалы автора, заглавие книги. Место издания, издательство, год издания, количество страниц книги.

Сведения о статье из периодического издания включают фамилию и инициалы автора, заглавие статьи, наименование издания, наименование серии, год выпуска, о том (при необходимости), номер издания, страницы, на которых помещена статья.

Не рекомендуется включать в библиографический список те источники, на которые нет ссылок в тексте пояснительной

записки и которые фактически не были использованы автором при работе над бакалаврской работой.

При цитировании или заимствований формул, графиков, методов расчета, таблиц и т.п. должны быть сделаны ссылки на источник: порядковый номер источника в библиографическом списке в квадратных скобках.

При необходимости сделать ссылки на стандарты, технические условия, инструкции и другие подобные документы.

Ссылаются на документ в целом или на его разделы с указанием обозначения и наименования документа, номера и наименование раздела. Ссылка на отдельные разделы, пункты и иллюстрации не допускается.

Правильно показанные источники дают возможность в некоторой степени оценить объем и глубину проработки темы, уровень научности и современности использованных методов и математического аппарата, в какой мере студент — проектант использовал руководящие документы, как он знаком с новейшей литературой по теме.

2.7. Стилистические рекомендации

Сокращение слов в тексте, как правило, не допускается, за исключением общепринятых: мм, кг, и другие единицы измерения, п. (пункт), ст. (статья) и т.п.

Если автором применяются не общепринятые сокращения, символы и термины, их перечень включается в пояснительную записку в тех случаях, когда их общее количество более 20 и каждое из них повторяется в тексте не менее 3—5 раз. Сокращения, символы и термины располагаются в перечне столбца, в котором слева приводится принятое сокращение, а справа — его детальная расшифровка.

При первом упоминании в тексте иностранных фирм, мало известных фамилий или географических названий их пишут, как в русской транслитерации, так и на языке

оригинала. Система условных и сокращенных обозначений должна быть единой по всей работе.

Пояснительная записка должна быть написана технически и литературно грамотным в третьем лице единственного числа.

В пояснительной записке не должно быть неясных формулировок, неоправданного повторении одних и тех же выражений, неправильного порядка слов, однообразия оборотов речи.

Следует избегать длинных фраз, вульгаризмов, канцелярских оборотов. Фраза должна быть краткой и ясной.

При разработке правил или инструкций следует использовать глаголы в повелительном наклонении или в неопределенно форме, чтобы исключить толкование об обязательности или необязательности конкретного пункта.

Нужно писать: в) произвести ...; г) проверить ...; з) пробовать ... и т.д. Причем начинать все пункты следует с глагола.

Необходимо избегать лишних слов и выражений: имеющие место; путем; со стороны; в деле; в порядке; либо, ... либо; или, ... или; по сути дела и т.д.

Не следует употреблять при существительных с количественными числительными общих определений и лишних слов, например, в декабре месяце, надо — в декабре; заменять сложные союзы: «для того, чтобы», союзом «чтобы», если на первой части этих слов нет логического ударения (именно, только).

Предлог «благодаря» не следует употреблять в случаях, когда речь идет о причинах, вызывающих нежелательный результат, например, нельзя — «благодаря оплошности сотрудника произошла утечка информации».

Слово «согласно», «вопреки», «благодаря» требуют дательного падежа, например: согласно приказу, вопреки обещанию, благодаря командиру. Надо правильно употреблять выражения «с помощью» и «при помощи», например: с помощью техники, при помощи специалистов.

Действительные обороты речи следует предпочитать страдательным, например: студенты разработали проекты, а не студентами были разработаны проекты.

Не нужно допускать выражений: текущего года, прошлого года, сего года. Годы следует указывать цифрами.

Следует:

- избегать употребления глаголов «производить», «осуществлять», «подвергать» в сочетании с существительными;

- давать прямую глагольную форму, например: испытывать, а не производить испытание, контролировать, а не осуществлять контроль, проверять, а не подвергать проверке;

- избегать не соподчинения главного и придаточного предложений, не смешивать настоящее и прошедшее время, совершенный и несовершенный вид, личную и безличную форму.

2.8. Оформление текстового материала

При написании курсовой работы необходимо использовались ГОСТы:

- ГОСТ 2.105-95. ЕСКД. «Общие требования к текстовым документам» (с обновлением на 13. 01. 2010 г.);

- ГОСТ 7.32-2001 «Отчет о научно-исследовательской работе. Структура и правила оформления»;

- ГОСТ Р 6.30-2003 «Унифицированная система документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов.»;

- ГОСТ 7.1-2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления»;

- ГОСТ 7.12-77 «Сокращение русских слов и словосочетаний в библиографическом описании»;

- ГОСТ 7.11-78 «Сокращение слов и словосочетаний на иностранных языках в библиографическом описании»;

- ГОСТ 7.80-2000 «Библиографическая запись. Заголовок. Общие требования и правила составления»;
- ГОСТ 7.82-2001 «Библиографическое описание электронных ресурсов: общие требования и правила составления»;
- ГОСТ 7.0.5-2008 «Библиографическая ссылка. Общие требования и правила составления».

Общие требования к оформлению работы

Согласно ГОСТ 7.32-2001 «Отчет о научно-исследовательской работе. Структура и правила оформления», текст печатается на одной стороне листа белой бумаги формата А4 через полтора интервала. Работа брошюруется.

Цвет шрифта — черный. Размер шрифта (кегель) 12 или 14. Тип шрифта — *Times New Roman*. Шрифт печати должен быть прямым, четким, черного цвета, одинаковым по всему объему текста. Разрешается использовать полужирный шрифт при выделении заголовков структурных частей курсовой (дипломной) работы (оглавление, введение, название главы, заключение и т.д.). Текст обязательно выравнивается по ширине.

Размер абзацного отступа — 1,5 см.

Страница с текстом должна иметь левое поле 30 мм (для сшивания в дело), правое — 10 мм, верхнее и нижнее 20 мм (ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов»).

Страницы работы нумеруются арабскими цифрами (нумерация сквозная по всему тексту). Номер страницы ставится в центре верхнего поля листа без точки. Тип шрифта — *Times New Roman*.

Титульный лист входит в общую нумерацию, но номер на нем не ставится. Все страницы, начиная со второй (Содержание), нумеруются.

В тексте используется «длинное тире», его клавиатурное сочетание в *MS Word* — *Ctrl + Alt +* минус на дополнительной клавиатуре.

Используются «кавычки — елочки», для вложенных кавычек — „кавычки-лапочки”.

Рекомендуется разделы начинать с новой страницы. Заголовки разделов располагают в середине строки, оформляют прописными буквами без переноса слов, подчеркивания и точки в конце. Если заголовок подразделов, пунктов и подпунктов начинают с абзацного отступа и печатают строчными буквами, кроме первой прописной, не подчеркивают и не ставят точку в конце. Заголовки от основного текста определяют не менее чем одной пустой строкой. Подчеркивать и переносить слова в заголовках не допускается. Межстрочный интервал между последовательными заголовками выбирается таким, как в основном тексте.

Не допускается размещать наименование раздела, подраздела, а также пункта и подпункта в нижней части страницы, если после него расположена только одна строка текста.

В тексте буквенные обозначения физических величин должны соответствовать государственным стандартам. При расчете необходимо пользоваться системой единиц СИ, а при указании единиц величин соблюдать требования ГОСТ «Единицы физических величин» (ГОСТ 8.417-81).

Формулы и уравнения располагают и центрируют в отдельных строках непосредственно после текста, в котором они упомянуты. До и после формулы или уравнения необходимо пропустить не менее одной пустой строки. Нумеруют формулы и уравнения сквозной нумерацией в пределах всей ПЗ в круглых скобках на уровне формулы или уравнения, в крайнем правом положении на строке. Пояснения значений символов и числовых коэффициентов производят в «Перечне условных обозначений», приводимом в начале ПЗ. Для неучтенных обозначений непосредственно под формулой

или уравнением производят их пояснения. Пояснения для каждого символа следует давать с новой строки в той последовательности, в которой они встречаются. Первую строку пояснений начинают словом «где» без двоеточия. Например: «Среднюю скорость выхода газо-воздушной смеси из устья источника выброса можно определить по формуле»

$$W = \frac{4V_1}{\pi D^2}, \quad (1)$$

где D — диаметр устья;

V_1 — объем газо-воздушной смеси;

Перенос формулы или уравнения на следующую строку допускается только на знаках выполняемых операций; знак операции повторяется на следующей строке. Последовательно идущие формулы или уравнения разделяются точкой с запятой.

Ссылки в тексте на формулы необходимо давать в круглых скобках, (...). Не следует их путать со ссылками на литературные источники, которые делаются в квадратных скобках, т.е. []. Например: «Из (1) видно, что... » [4].

Примерный объем курсовой работы 30—40 страниц. В этот объем включается: титульный лист, содержание, введение, основной текст, заключение, библиографический список.

Приложения в общий объем не включаются.

Первым листом работы является титульный лист, оформляемый в соответствии с прилагаемым образцом (Приложение А).

Оформление заголовков

Заголовки структурных элементов работы располагают в середине строки (выравнивание по центру), без точки в конце и печатают заглавными буквами (*Caps Lock*) без подчеркивания. Каждый структурный элемент и каждую новую главу следует начинать с новой страницы.

Шрифт заголовков — *Times New Roman*, полужирный.

Размер шрифта:

1. Заголовок (главы, название раздела) — 16 (заголовок первого уровня)

1.1. Заголовок — 15 (заголовок второго уровня)

1.1.1. Заголовок — 14 (заголовок третьего уровня)

Разделы нумеруют. Разделы могут делиться на подразделы и пункты. Номер подраздела состоит из номеров раздела и номера подраздела в разделе (например, 1.2 (1 — номер раздела, 2 — номер подраздела), 2.5 (2 — номер раздела, 5 — номер подраздела) и т.д.), разделенных точкой. В конце номера точка ставится. Аналогичным образом нумеруются и пункты (например, 2.4.2. Анализ результатов). В нумерации после цифр идет пробел, а не табуляция. Заголовки разделов и подразделов следует печатать с абзачного отступа с прописной буквы, без точки в конце, не подчеркивая. Если заголовок первого уровня не помещается на одной строке, то на нижнюю строку переносят слово полностью. Разрыв слов при переносе не допускается. Между текстом и заголовком второго и третьего уровня оставляют двойной межстрочный интервал.

Заголовки второго и третьего уровней выделяют полужирным.

Оформление содержания

На втором листе помещается содержание, где указываются основные разделы работы и соответствующие им страницы. Заголовок СОДЕРЖАНИЕ пишется заглавными буквами посередине строки. Содержание включает введение, наименование всех глав, разделов и подразделов, заключение, библиографический список, приложения, с указанием номеров страниц, с которых начинаются эти элементы работы. По ГОСТ 2.105-95 наименования, включенные в содержание, записывают строчными буквами, начиная с прописной буквы, допускается набор заголовков первого уровня заглавными буквами. Текст должен соответствовать содержанию, как по содержанию, так и по форме.

Оформление рисунков

К рисункам относятся все графические изображения (схемы, графики, фотографии, рисунки). На все рисунки в тексте должны быть даны ссылки.

Рисунки должны располагаться непосредственно после текста, в котором они упоминаются впервые, или на следующей странице. Рисунки нумеруются арабскими цифрами, при этом нумерация сквозная, но допускается нумеровать и в пределах раздела. В последнем случае номер рисунка состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой (например: Рисунок 1.1). Название пишется под рисунком по центру, как и рисунок, форматирование — как и у обычного текста. Слово «Рисунок» пишется полностью. Если рисунок один, то он обозначается «Рисунок 1». Допускается не нумеровать мелкие иллюстрации (мелкие рисунки), размещенные непосредственно в тексте и на которые в дальнейшем нет ссылок. При ссылках на иллюстрацию следует писать «... в соответствии с рисунком 2» при сквозной нумерации и «... в соответствии с рисунком 1.2» при нумерации в пределах раздела, или (Рисунок 1.). После слово «Рисунок 2» пишется название. В этом случае подпись должна выглядеть так: «Рисунок 2 — Название». Точка в конце названия рисунка не ставится. Если в работе есть приложения, то рисунки каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением впереди обозначение приложения (например, Рисунок А.3).

Оформление таблиц

Цифровой материал в пояснительной записке рекомендуется оформлять в виде таблиц и приводить только значащие цифры: Таблицы применяют для лучшей наглядности и удобства сравнения показателей.

На все таблицы в тексте должны быть ссылки. Таблица должна располагаться непосредственно после текста, в котором она упоминается впервые, или на следующей странице. Все таблицы нумеруются (нумерация сквозная, либо в пределах

раздела — в последнем случае номер таблицы состоит из номера раздела и порядкового номера внутри раздела, разделенных точкой (например: Таблица 1.2). Таблицы каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением впереди обозначения приложения (например: Таблица В.2). Слово «Таблица» пишется полностью. Наличие у таблицы собственного названия обязательно. Название состоит из «Таблицы», номера, тире и названия. Название таблицы следует помещать над таблицей слева, без абзацного отступа в одну строку с ее номером через тире (например: «Таблица 3 — Название»). Точка в конце названия не ставится.

Заменять кавычками повторяющиеся в таблице цифры, математические знаки, знаки процента и номера, обозначение марок материалов и типоразмеров изделий, обозначения нормативных документов не допускается.

При отсутствии отдельных данных в таблице следует ставить прочерк (тире).

При переносе таблицы на следующую страницу название помещают только над первой частью, при этом нижнюю горизонтальную черту, ограничивающую первую часть таблицы, не проводят. Над другими частями также слева пишут слово «Продолжение» и указывают номер таблицы (например: Продолжение таблицы 1).

Заголовки столбцов и строк таблицы следует писать с прописной буквы в единственном числе, а подзаголовки столбцов - со строчной буквы, если они составляют одно предложение с заголовком, или с прописной буквы, если они имеют самостоятельное значение. В конце заголовков и подзаголовков столбцов и строк точки не ставят. Заголовки столбцов, как правило, записывают параллельно строкам таблицы, но при необходимости допускается их перпендикулярное расположение.

Горизонтальные и вертикальные линии, разграничивающие строки таблицы, допускается не проводить, если их отсутствие не затрудняет пользование таблицей. Но

головка таблицы должна быть отделена линией от остальной части таблицы.

При ссылке на таблицу следует писать: «Анализ таблицы 3 показывает ...» или «Анализ табл. 3 показывает ...»

Оформление приложений

В тексте проекта на все приложения должны быть даны ссылки. Приложения располагают в порядке ссылок на них в тексте. Каждое приложение следует начинать с новой страницы с указанием наверху посередине страницы слова «Приложение» и его обозначения. Приложение должно иметь заголовок, который записывают симметрично относительно текста с прописной буквы отдельной строкой. Приложения обозначают заглавными буквами русского алфавита, начиная с А, за исключением букв Ё, З, Й, О, Ч, Ъ, Ы, Ь. После слова «Приложение» следует буква, обозначающая его последовательность (например: Приложение Б). Допускается обозначение приложений буквами латинского алфавита, за исключением букв I и O. Если в работе одно приложение, оно обозначается «Приложение А»

Текст каждого приложения может быть разделен на разделы, подразделы и т.д., которые нумеруют в пределах каждого приложения. Перед номером ставится обозначение этого приложения. При этом нумерация страниц приложений и основного текста должна быть сквозная.

Оформление ссылок и сносок

При написании проекта студенту часто приходится обращаться к цитированию работ различных авторов, использованию статистического материала. В этом случае необходимо оформлять ссылку на тот или иной источник. При цитировании необходимо соблюдать следующие правила:

— текст цитаты заключается в кавычки и приводится в той грамматической форме, в какой он дан в источнике, с сохранением особенностей авторского написания.

— цитирование должно быть полным, без искажения смысла.

Пропуск слов, предложений, абзацев при цитировании допускается, если не влечет искажение всего фрагмента, и обозначается многоточием, которое ставится на месте пропуска.

— каждая цитата должна сопровождаться ссылкой на источник, библиографическое описание которого должно приводиться в соответствии с требованиями библиографических стандартов.

Библиографическая ссылка является частью справочного аппарата курсовой работы и служит источником библиографической информации о документах — объектах ссылки. Объектами составления библиографической ссылки являются все виды опубликованных и неопубликованных документов на любых носителях, а также составные части документа.

Оформление библиографического списка

Библиографическое оформление проекта (ссылки, библиографический список) выполняется в соответствии с едиными стандартами по библиографическому описанию документов: ГОСТ 7.1-2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления»; ГОСТ 7.12-77 «Сокращение русских слов и словосочетаний в библиографическом описании»; ГОСТ 7.11-78 «Сокращение слов и словосочетаний на иностранных языках в библиографическом описании»; ГОСТ 7.80-2000 «Библиографическая запись. Заголовок. Общие требования и правила составления»; ГОСТ 7.82-2001 «Библиографическое описание электронных ресурсов: общие требования и правила составления»; ГОСТ 7.0.5-2008 «Библиографическая ссылка. Общие требования и правила составления».

Каждая библиографическая запись в списке получает порядковый номер и начинается с красной строки. **Нумерация источников в библиографическом списке сквозная.**

Сведения о книгах (монографиях, учебниках, справочниках) включают в себя: фамилию, инициалы авторов, заглавие книги, место издания, издательство (или издание), год издания и общее количество страниц. Если авторов более трех, допускается указывать фамилии только трех из них и далее писать «и др.».

Сведения о статье из периодического издания содержат фамилию и инициалы автора, написавшего статью, ее название, название журнала (газеты), год, номер (для журнала), число (для газеты), первую и последнюю страницы, на которых помещена статья. Издательство указывают только для разовых сборников.

Сведения о стандартах включают в себя обозначения и наименования стандартов.

Сведения об изобретениях — регистрационный номер патента (авторского свидетельства), название страны (полное наименование), инициалы и фамилии авторов, издание, в котором опубликовано описание, год издания и номер выпуска информационного бюллетеня.

Сведения о проектной и другой технической документации должны содержать: заглавие, вид документации, организацию, выпустившую документацию, город и год выпуска.

Библиографические описания в библиографическом списке рекомендуется приводить в алфавитном порядке.

В тексте пояснительной записки должны быть ссылки на источники из библиографического списка. При этом номер источника из библиографического списка указывают в квадратных скобках, (например, «В [2 — 7] отмечается ...»). Ссылки на неопубликованные материалы запрещаются!

Излагать текст пояснительной записки предпочтительно в безличной форме (например, «...для уменьшения влияния акустических каналов утечки информации в помещении применены звукопоглощающие покрытия»). Допускается излагать текст от первого лица множественного числа (например: «... выполняя расчет опасности каналов утечки

информации, используем экспертную оценку...»). Не принято излагать текст от первого лица единственного числа.

В пояснительной записке должны быть применяемы научно-технические термины, обозначения и определения, установленные соответствующими стандартами, а при их отсутствии — общепринятые в научно-технической литературе. Если в пояснительной записке принята специфическая терминология, то она должна быть отражена в перечне условных обозначений, символов, единиц, сокращений и терминов с соответствующими разъяснениями.

В тексте пояснительной записки не следует применять не принятые в литературе сокращения («т.о.», вместо «таким образом» и т.п.). Все сокращения должны соответствовать русской орфографии и нормам стандартов. Нельзя также применять буквенные и другие сокращения без приведения понятий (t , R , $\min$, % и т.п.). Например, нельзя написать «Значение t » вместо «значение температуры t ». В таблице разрешается пользоваться символами, при условии их расшифровки в тексте, поясняющем таблицу, либо в списке сокращений.

При изложении расчетов не следует применять табличную форму. В общем случае расчет какого-либо параметра должен содержать:

- наименование параметра;
- его буквенное обозначение;
- расчетную формулу в буквенном виде;
- расчетную формулу после подстановки в неё численных значений величин;
- численное значение расчетной величины;
- ее размерность.

Оформление графического материала

Демонстрационный материал должен иллюстрировать и пояснять пояснительную записку проекта. Чертежи и таблицы, кроме того, должны наглядно отражать умение студента-проектанта составлять графические документы.

Не допускается увеличение объема графических работ за счет простейших схем или чертежей, не отражающих существа работы. Чертежи должны строго соответствовать действующим ГОСТам.

Независимо от вида чертежи на листах чертежной бумаги должны быть строго определенных размеров. Размер листа зависит от номера формата, выбранного из номенклатуры форматов. Форматы разделяются на основные и дополнительные и определяются размерами внешней рамки, выполняемой тонкой линией.

Основной формат для чертежей курсовой работы — А4. В случае необходимости допускаются другие чертежные форматы. Графические документы всех видов должны быть выполнены линиями, форма и толщина которых соответствуют ГОСТ 2.303-68.

Основная надпись для чертежей и схем выполняется в правом нижнем углу документа сплошными основными и сплошными тонкими линиями. На листах формата А4 основные надписи располагают вдоль короткой стороны листа.

Наименования, заголовки, обозначения в основной надписи допускается писать без наклона. Надписи и буквенные обозначения, относящиеся к видам, разрезам, сечениям и выносным элементам, должны быть расположены параллельно основной надписи чертежа над соответствующим изображением.

В основной надписи для заголовков рекомендуется использовать шрифты размеров 7 или 10, для остальных — 3,5. Обозначения следов секущих плоскостей необходимо выполнять шрифтами размеров 7 или 10, нанесение позиций на сборочных чертежах — шрифтами размеров 5 или 7.

Чертежи узлов, агрегатов и так далее должны иметь проекции, разрезы и сечения, полностью поясняющие идею и вид конструкции, а также габаритные основные размеры и размеры, полученные из расчетов.

При выполнении схем и карт, графических планов, схем взаимодействия руководствоваться требованиями правил

оформления документов, а также наставлений по делопроизводству.

Каждый элемент, входящий в изучение и изображенный на схеме, должен иметь буквенно-цифровое позиционное обозначение. Каждая схема должна иметь перечень элементов.

Для обеспечения иллюстративности доклада может потребоваться схема (плакат) в цветном изображении. В этом случае для раскраски используются не более шести цветов.

2.9. Подготовка к защите курсового проекта

Это завершающая часть курсового проекта, называемое защитой.

Руководителю проекта предъявляется пояснительная записка, чертежи (плакаты), демонстрирующий макет (презентацию) и сам доклад по курсовому проекту. Продолжительность доклада 5—7 минут.

Доклад включает:

- полное название темы;
- обоснование ее актуальности;
- формулировку инженерной задачи;
- характеристику алгоритма, обеспечивающего ее решение;
- демонстрацию работы алгоритма на конкретном примере;

Приложение А.
ОБРАЗЕЦ ОФОРМЛЕНИЯ ТИТУЛЬНОГО ЛИСТА

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВО «Севастопольский государственный университет»
Институт радиоэлектроники и информационной безопасности
Кафедра информационной безопасности

Курсовой проект по дисциплине
«Основы информационной безопасности»

Выполнил
студент группы ИБ/б-31-о
Фамилия, имя, отчество

Допущен к защите
Защищен с оценкой
«__» _____

Руководитель проекта
«__» _____

фамилия, инициалы

Севастополь
2015

Приложение Б.
ОБРАЗЕЦ ЗАДАНИЯ НА КУРСОВОЙ ПРОЕКТ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования «Севастопольский
государственный университет»

Институт радиоэлектроники и информационной безопасности
Кафедра информационной безопасности

Направление подготовки / специальность: 10.03.01 —
Информационная безопасность

Профиль/специализация _____

Курс _____ Группа _____ Семестр _____

ЗАДАНИЕ
НА КУРСОВОЙ ПРОЕКТ (РАБОТУ) СТУДЕНТА

(фамилия, имя, отчество студента)

1. Тема проекта (работы): **исследование каналов утечки информации для объекта информатизации**

2. Сроки сдачи студентом законченного проекта (работы) _____

3. Исходные данные к проекту (работе):

6. Дата выдачи задания « » 201 г.

[illegible]

[illegible]

Студент _____ (подпись)

Руководитель проекта
(работы) _____
(фамилия, инициалы, должность) (подпись)

« _____ » 20 ____ г.

Приложение В.

ОБРАЗЕЦ ВЫПОЛНЕНИЯ КУРСОВОГО ПРОЕКТА

ВВЕДЕНИЕ

Актуальность темы. Информация, как совокупность знаний о фактических данных и зависимостях между ними, стала стратегическим ресурсом, она является обязательным сырьем для выработки любого решения, без чего самые лучшие планы останутся простым самообманом и будут обречены на неудачи. Техническими средствами освоения этого ресурса выступают вычислительные машины с их разнообразным оборудованием и сети связи. Кроме того при переходе к рыночной экономике информация также становится товаром и должна поэтому подчиняться специфическим законам товарно-рыночных отношений. В этих условиях проблема защиты информации, другими словами коммерческой тайны является весьма актуальной и для организаций любой формы собственности.

Специалисты относят к понятию коммерческой тайны любую конфиденциальную управленческую, научно-техническую, торговую и другую информацию, представляющую ценность для предприятия в достижении преимущества над конкурентами и извлечения прибыли, утечка этой информации может нанести ущерб ее владельцам в виде прямых убытков или упущенной выгоды. Высокая уязвимость информационных технологий к различным злоумышленным действиям породило острую необходимость в средствах противодействия этому, что привело к возникновению и развитию области защиты информации как неотъемлемой части информационной индустрии.

Цель и задачи работы. Изучить каналы утечки информации для объекта информатизации расположенного в помещении № 419.

Задачи, которые необходимо решить для достижения поставленной цели:

- проанализировать рассматриваемый объект, составить генеральный план ОИ и ситуационный план;
- разработать модели угроз;
- произвести оценку рассмотренных каналов утечки информации.

Структура работы. Курсовой проект состоит из: введения, списка условных сокращений, определений, 3 разделов, библиографического списка и заключения.

1. ОПИСАНИЕ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Описание здания, где расположен объект информатизации

Адрес здания, где расположен объект ОИ: Севастополь, улица Курчатова, 7.

Здание жилое, четырехэтажное. Фундамент здания — железобетонный, стены — известняк. Перекрытие между этажами выполнено из железобетонных плит. Кровля здания — плоская крыша из плит перекрытия и рубероида, без чердачного помещения. Полы залиты цементной стяжкой, сверху деревянный настил, покрытый линолеумом. Фасад здания ориентирован на запад.

Электроснабжение — центральное. Системы теплоснабжения осуществляется от котельной расположенной на территории университета. Канализации и водоснабжения — общегородские.

Телефонизация здания, а также интернет осуществляется от технологического оборудования ОАО «Севтелеком» и не имеет выхода на город. Связь проходит через общ. 1, 2, 3, 4 (приложение Г поз. 1, 2, 3, 4) и здания расположенные на территории института ЯЭиП, являющегося структурным подразделением СевГУ.

Вход в здание осуществляется с двух входов, расположенных с западной стороны здания. Также вход может осуществляться с южной стороны, но данная часть здания является территорией военной части. Непосредственно функциональная часть общежития находится на 3 и 4 этаже

здания и вход в него контролируется сотрудником университета. Существует пропускной режим ограниченное время посещения с 6.00 до 11.00.

Охрана здания производится сотрудниками университета, а также сотрудниками специальной комендатуры охраны ядерного реактора.

За пределы здания выходят:

- трубы водяного отопления;
- линии электропитания;
- трубы холодной и горячей воды системы водоснабжения;
- трубы канализации;
- линия внутренней телефонной связи;
- радиоканалы сотовой связи;
- интернет связь.

Описание и характеристики помещения

Генеральный план объекта информатизации приведен в Приложении Д.

Объект защиты представляет собой жилую трехместную комнату общежития, которая расположена на 4 этаже четырехэтажного здания. Комната предназначена для проживания иногородних студентов СевГУ. Площадь рассматриваемого помещения равна 16 м².

Стены: несущие стены выполнены из кирпича, стена со смежными комнатами (южная и северная сторона) из известняка, оштукатурена и окрашена водо-дисперсионной краской. Толщина стен: восточная — 350 мм, северная — 150 мм, западная — 150 мм, южная — 150 мм.

Потолок выполнен из пустотелых плит перекрытия, шпатлевки и побелки. Крыша прямая, покрыта рубероидом.

Окно (приложение Д, поз. 23): рама выполнена из древесины. Окно имеет двойное остекление, имеют двойную форточку. Стекло толщиной 3 мм, закреплено деревянными штапиками в раме. На окне имеются металлические запорные устройства в виде шпингалетов.

Дверь (приложение Д поз. 18): стандартная, комнатная, выполнена из древесины и обшита ДВП. Имеется запорное устройство в виде врезного английского замка. Рама дверная выполнена из дерева с порогом. Дверной глазок отсутствует.

В помещении находятся система электропитания и освещения, которая запитана через распределительный щиток, расположенный в коридоре, возле помещения № 401. На распределительном щитке отсутствует запорное устройство. Доступ к нему не ограничен.

Описание смежных комнат:

- с западной стороны — жилая комната № 417
- с восточной стороны — жилая комната № 421
- с южной стороны — коридор
- с северной стороны — окно (приложение Б поз. 23)
- сверху — крыша общежития
- снизу — жилая 3 местная комната 319, аналогично

объекту информационной деятельности.

Описание ситуационного плана объекта информатизации

Ситуационный план приведен в приложении Г.

Исследуемый объект ИОД расположен в северо-восточной части города. С северной стороны на расстоянии 30 метров расположено жилое здание — объект № 9. С северо-востока на расстоянии 70 метров — территория университета. С восточной стороны здание окружено проезжей частью на расстоянии 40 метров и территорией университета — 50.

С юга на расстоянии 20 метров расположен объект № 2.

С юго-запада — 80 метров деревья высотой 12 метров с запада — 150 метров объект № 5. С северо-западной стороны расположен объект № 8 на расстоянии 200 метров.

Основные сведения об объектах расположенных в непосредственной близости со зданием, в котором расположен ОИ, приведены в таблице 1.

Таблица 1 — Основные сведения об объектах, расположенных
вблизи исследуемого здания

№	Наименование объекта	Кол-во этажей	Адрес	Характеристика объекта	Расстояние до ОИ, м
1	2	3	4	5	6
1	Общежитие №3	4	Курчатова	Здание, в котором расположен исследуемый ОИ	—
2	Общежитие №2	4	Курчатова	Жилое здание, предназначенное для проживания студентов	20
3	Общежитие № 1	4	Курчатова	Жилое здание, предназначенное для проживания студентов	50
4	Общежитие №4	4	Курчатова	Здание не жилое, в процессе постройки	80
5	Черное море	—	—	—	15 0
6	Лодочная	2	Курчатова	Объект на данный момент не функционирует	80
7	Плац	—	—	—	40
8	Спортивная площадка	—	—	Объект является общим для все проживающих общежитий	20
9	Семейное общежитие	4	Курчатова	Здание жилое, предназначенное для проживания сотрудникам университета	20
10	Башни	—	Курчатова	Предназначенные для хранения воды, расположены с восточной стороны	20
11	Котельная	1	Курчатова	—	25
12	Проезжая часть	—	—	—	70
13	Технический корпус	1	Курчатова	—	80

Продолжение таблицы 1

1	2	3	4	5	6
14	Санитарный узел	2	Курчатова	Предназначен для приема и осмотра студентов и сотрудников университета	40
15	Контрольно - пропускной пункт	—	Курчатова	Обеспечивает охрану территории университета и контроль за входом в университет	40
16	Аудиторное помещение СНУЯ и П (300/1/2)	2	Курчатова	—	45
17	Контрольно - пропускной пункт	—	Курчатова	Обеспечивает охрану территории университета и контроль за входом в университет	60
18	Жилой дом	5	Курчатова		15 0
19	Остановка		Курчатова		14 0

Технические средства

Схема размещения технических средств представлена в Приложении Д.

Вспомогательные технические средства. К вспомогательным техническим средствам относятся: технические средства открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, радиотрансляции, электробытовые приборы и т.д., а также элементы интерьера внутри помещения. В таблице 2 приведены сведения об элементах интерьера рассматриваемого помещения.

Таблица 2 — Элементы интерьера помещения № 419

№	Наименование технического средства	Позиция	Количество
1	кровать	1,2,3	3
2	тумбочка	7,8,13,17	4
3	стол	9,4	2
4	шкаф	5	1
5	холодильник	6	1
6	стулья	10,11,16,15	4
7	батарея	12	1
8	дверь	18	1
9	розетки	24,22,21,20	4
10	выключатель	19	1
11	окно	23	1
12	люстра	14	1 (на 4 лампочки)

Основные технические средства. Основными объектами защиты информации являются:

— информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;

— средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звуко-сопровождение, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), их информативные физические поля.

В рассматриваемом ОИ таким средством является ноутбук, на котором происходит непосредственная обработка

информации, расположенный на тумбочке (поз. 13). Другие ОТС в данном помещении отсутствуют.

2. КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Акустические каналы утечки информации

Данный вид канала утечки информации может быть создан путем непосредственного прослушивания разговоров в исследуемом помещении без применения специальных технических средств.

Данный способ прослушивания возможно осуществить в коридоре описанного выше здания, следующими лицами: сотрудниками университета или посетителями в рабочее время, а также проживающими данного общежития как в рабочее, так и не в рабочее время. Но из коридора прослушивание, будет осложнено тем, что коридор проходит через все здание и злоумышленник рискует быть замеченным.

Также возможно прослушивание разговоров, лицом, находящимся в соседнем помещении (комната № 421, № 417). Этот способ более эффективен, так как обнаружить злоумышленника практически невозможно, а качество полученной информации будет довольно высокой, так как в исследуемом помещении плохая звукоизоляция стен.

Прослушивание разговоров с помощью закладных и записывающих устройств.

Закладные, записывающие устройства могут быть установлены как сотрудниками университета, посетителями в рабочее время, так и проживающими в рабочее и нерабочее время. Существуют несколько позиций (рис. 2.1), подходящих для установки данных устройств, наиболее приближенных к носителю нужной информации, так как в данном помещении проживают 3 человека, проводить закладку необходимо максимально близко к интересующему лицу, во избежание большого количества шумов и искажения информации. Такими позициями являются (приложение Ж): кровать (поз. 3), тумбочки (поз. 13,8,7), подоконник (поз. 23), батарея (поз. 12), стол (поз. 4), розетка (поз. 22).

Данный способ прослушивания имеет преимущество, по сравнению с остальными, а именно: возможность записи разговора на носитель и дальнейшего его использования и изучения в не помещения. Его недостатком является ограниченная продолжительность записи, и необходимость повторного проникновения в помещения для изъятия устройства.



Рисунок 2.1 — Размещение закладных устройств

Прослушивание с помощью направленного микрофона.

Установка направленного микрофона возможно на башнях (приложение Г, поз. 10) расположенных непосредственно напротив окна на расстоянии 20 метров. Но произвести установку на данном объекте постороннему лицу практически невозможно. Так как за башнями ведется круглосуточное наблюдения сотрудниками воинской части, расположенной на первом этаже рассматриваемого здания. Поэтому установку с целью получения информации в этом случае может осуществить только сотрудник воинской части. Так же для прослушивания этим способом необходимо наличие открытого окна.

Направленный микрофон также можно установить на дерева (приложение Г, поз. 1).

Данный вид микрофона возможно применить также с использованием телескопической штанги. Сотрудник воинской части расположенной на первом этаже общежития может в темное время суток воспользоваться этими устройствами для получения информации, аналогично применить данные устройства может и человек находящийся в соседних помещениях, через открытое окно (приложение Д, поз.23).

Проводные микрофоны

Установка проводных микрофонов возможна из коридора или из соседних помещений сотрудниками университета, посетителями в рабочее время или проживающими общежития. Можно установить прослушивающее устройство из соседних комнат № 421 и № 417, так как не качественно была сделана электропроводка по зданию, а также из-за размера толщины южной стены.

Оценка угрозы:

— время необходимое для осуществления канала утечки информации 4 часа, т.к. это минимальное время установки прослушивающего оборудования учитывая время занятия необходимой позиции;

— время необходимое для нахождения канала утечки информации – 1 часа учитывая площадь помещения и возможные места расположения оборудования;

— время для ликвидации канала утечки информации (для изъятия устройства) — 10 минут.

Оценка возможности организации: **4**, т.к. для организации канала требуется много времени и средств.

Оценка привлекательности информации: **3**, т.к. акустическая информация, циркулирующая в помещении средне насыщенная, и не имеет большой смысловой ценность.

Оценка по степени, опасности полученной информации:
4.

Акустоэлектрические каналы утечки информации

Акустоэлектрические технические каналы утечки информации возникают в следствие преобразования информативного сигнала из акустического в электрический за счет «микрофонного» эффекта в электрических элементах вспомогательных технических средств и систем (ВТСС).

В рассматриваемом помещении, маловероятно реализовать акустоэлектрический канал утечки информации, в связи с отсутствием ВТСС, которые имеют «микрофонный эффект» (телефонная линия, пожарная сигнализация), а также отсутствие ВТСС с электромагнитным ВЧ-излучением, модулированным информативным звуковым сигналом.

Оценка угрозы

Оценка угрозы по данному каналу не производилась, вследствие отсутствия данного канала утечки информации

Виброакустический канал утечки информации

Образование виброакустического канала утечки информации происходит в следствии появления вибрационных колебаний в строительных и инженерных конструкциях, вызванных акустическим полем звука внутри помещения.

В данном случае колебания могут передаваться через (приложение Г):

- дверь (поз. 18);
- окно (поз. 23);
- система отопления (батарея (поз. 12));
- стены;

Установку устройств, с помощью которых происходит прием информации на основе вибрационных колебаний могут осуществлять сотрудники университета, посетители, а также проживающие в общежитии в рабочее и в не рабочее время.

Для перехвата речевой информации по виброакустическим каналам в качестве средств акустической разведки используются электронные стетоскопы и закладные устройства с датчиками контактного типа. Электронные стетоскопы и закладные устройства с датчиками контактного

типа позволяют перехватывать речевую информацию без физического доступа «агентов» в выделенные помещения. Их датчики могут быть установлены на наружных поверхностях здания, на оконных проемах и рамах, в смежных (служебных и технических) помещениях за дверными проемами, ограждающими конструкциями, на перегородках, трубах систем отопления и водоснабжения, коробах воздуховодов вентиляционных и других систем.

В исследуемом объекте данные устройства могут находиться:

— в соседних комнатах, при этом колебания будут сниматься с западной и восточной стены. Но установка в данных позициях стетоскопов усложнено тем, что эти помещения являются жилыми комнатами. И в этом случае «агентом» должен быть или проживающий в этой комнате, или посторонним, проникшим в данные помещения во время отсутствия ее владельцев. Также «агенту» необходимо будет установить в помещении дополнительно радиопередатчик, или диктофон, на который будет записываться информация, поступающая со стетоскопа. Но устанавливать стетоскопии на данных позициях не рационально, так как злоумышленнику необходимо будет повторно проникать в помещение для изъятия устройства, с целью не быть раскрытым. Оптимально применять данные позиции, только в случае если «агентом» является проживающие данных помещений.

— с улицы, при этом колебания будут сниматься с южной стороны стены помещения, а также с оконных рам (приложение Д, поз. 23) помещения. Это самый надежный и эффективный метод снятия информации, так как не требует проникновение ни в помещение, ни даже в само здание, и обнаружить такое устройство с наружной части стены практически невозможно. Связано это с небольшими размерами самого устройства и расположением помещения на четвертом этаже. Установка систем съема информации на данных позициях усложняется тем, что территория общежития

с данной стороны здания охраняется сотрудниками воинской части.

Оценка угрозы:

— время необходимое для организации канала утечки информации (для установки 1 час);

— время необходимое для обнаружения канала утечки информации для нахождения устройства — 2 часа для стетоскопов с учетом площади здания и размеров устройств;

— время для ликвидации канала утечки информации (для изъятия устройства — 10 минут).

Оценка возможности организации: **5**, т.к. имеется возможность устанавливать устройства на крыши соседних зданий.

Оценка привлекательности информации: **4**, т.к. эта информация акустическая.

Оценка по степени опасности: **3**, т.к. полученная таким способом информация представляет малую ценность.

Лазерный канал утечки информации

Лазерный акустический канал утечки информации основан на дистанционном перехвате вибрационных колебаний жестких поверхностей, которые возникают под влиянием акустического поля звука. Возможное расположение источника сигнала для лазерного канала утечки информации показано на рис.2.2. Для рассматриваемого помещения наибольшую опасность представляют ЛСАР, которые устанавливаются в зоне прямой видимости из окон комнаты (приложение Д, поз. 23).



Рисунок 2.2 — Возможное расположение источника сигнала для лазерного канала утечки информации

Учитывая расположение окна, местами размещения может быть:

- проезжая часть, находящаяся на возвышенности, на расстоянии 100 метров от рассматриваемого ОИ, практически напротив окна. Однако осуществления этого канала проблематично, потому что на предполагаемом месте установления лазера есть растительность, которая может помешать прохождению лазерного луча;

- башни (приложение Г, поз.10). Так как данные объекты расположены в зоне прямой видимости из окна, однако осуществление этого канала проблематично, потому что во время установки оборудования злоумышленник будет находиться в прямой видимости из окон жилых комнат общежития.

Возможные места расположения лазерных устройств съема информации показаны на рис.2.3.



Рисунок 2.3 — Возможные места расположения лазерных устройств съема информации

Учитывая городские условия и особенности расположения ОИ, наличие окон, вероятность применения ЛСАР является достаточно высокой.

Предельное расстояние для использования ЛСАР в городских условиях составляет около 200 метров.

Оценка угрозы:

— время необходимое для организации канала утечки информации (для установки 6 час);

— время необходимое для обнаружения канала утечки информации для нахождения устройства — 30 минут для стетоскопов с учетом площади здания и размеров устройств;

— время для ликвидации канала утечки информации (для изъятия устройства — 1 час).

Оценка возможности организации: **4**.

Оценка привлекательности информации: **4**, т.к. эта информация акустическая.

Оценка по степени опасности: **3**, т.к. полученная информация представляет малую ценность.

Визуально-оптические каналы утечки информации

Для данного объекта возможно три вида визуально-оптической утечки информации:

Снятие информации путем использования длиннофокусного оборудования. Данный вид утечки информации в рассматриваемом помещении возможно осуществить путем установки видеокамер на башнях (приложение А, поз.10), объекты, контролируемые с позиции 10 показаны на рис.2.4, и на холме возле проезжей части (приложение Г, поз. 12). Вид с места установки устройств съема видовой информации на холме показан на рис.2.5

Видеокамера, установленная на башнях позволит просматривать: кровать (приложение Д, поз. 3), стол (приложение Д, поз.4), тумбочку (приложение Д, поз. 7), стулья (приложение Д, поз. 10, 15, 16), шкаф (приложение Д, поз. 4). Для просмотра помещения с данной позиции необходима массивная длиннофокусная оптика, т.к. здание расположено на расстоянии 40 метров.

Возможна установка камеры в коридоре общежития с целью получения информации о наличии жильцов в помещении.

Установка длиннофокусной техники на холме (приложение Г, поз. 12) не целесообразна по причине наличие большого количества растительности, что затрудняет снятие информации.

Установка видеокамер из соседних помещений. При установке видеокамер из соседних помещений комната будет просматриваться идеально, но существуют не большие трудности при установки такой аппаратуры, то есть время которое займет установка затрудняет ее реализацию. В данном случае затрудняется реализация из-за толщины стен и визуального контроля помещений из которых будет вестись установка специальной техники. Исходя из вышеизложенного можно сказать, что соседние комнаты и коридор малопригодны для установки видеокамер.



Рисунок 2.4 — Объекты, контролируемые с позиции 10

Контроль со стороны персонала (невооруженным глазом).

Видеоконтроль со стороны персонала возможен жильцами общежития и посетителями. Возможно осуществить видеоконтроль находясь в коридоре при открытой двери (приложение Д, поз. 18). На рис. 2.6 показаны объекты, контролируемые злоумышленником при частично открытой двери, на рис. 2.7 показаны объекты, контролируемые злоумышленником при полностью открытой двери.

Также, установку видеокамер можно осуществить в нутрии рассматриваемого ОИ, посетителями, или сотрудниками университета, в рабочее и не рабочее время. В этом случае камера может быть установлена на шкафу (приложение Д, поз. 5). При таком расположении видеокамеры будут рассматриваться объекты, показанные на рисунке 2.8.

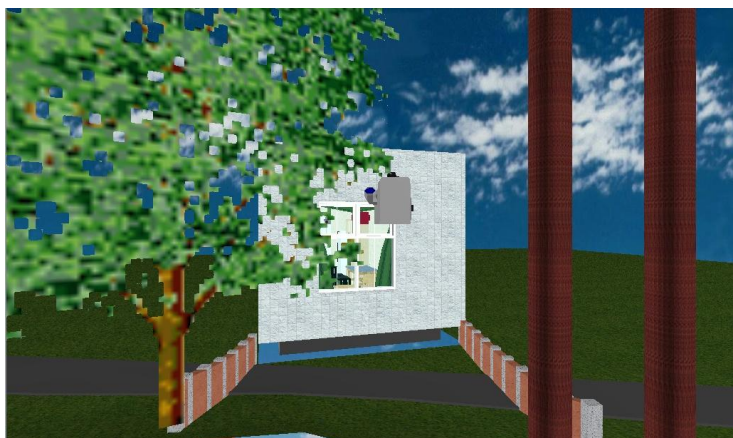


Рисунок 2.5 — Вид с места установки устройств съема
видовой информации на холме

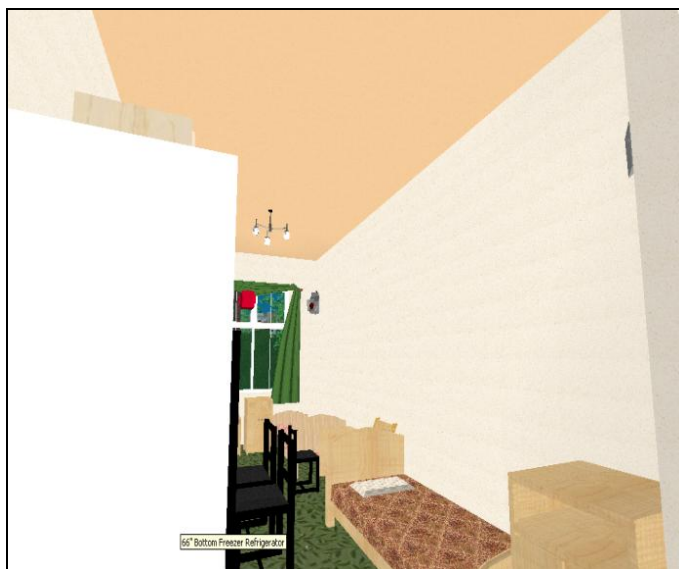


Рисунок 2.6 — Объекты, контролируемые злоумышленником
при частично открытой двери

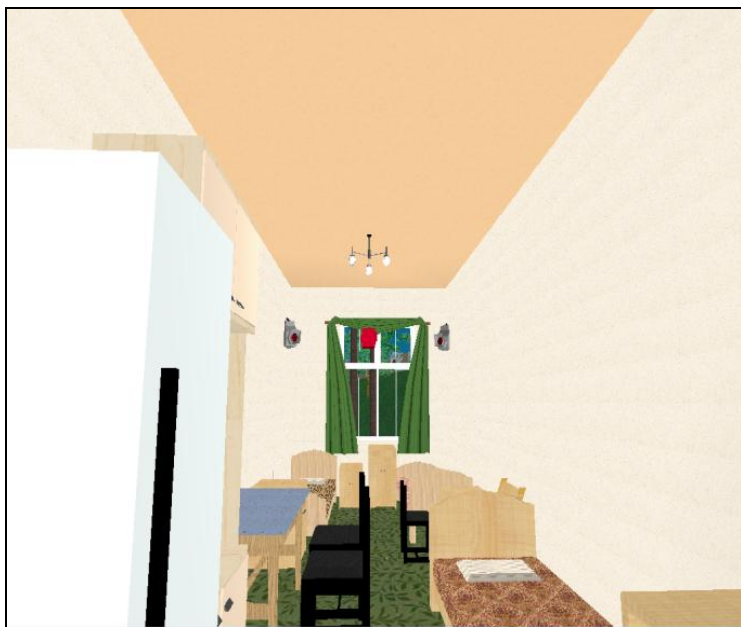


Рисунок 2.7 — Объекты, контролируемые злоумышленником при полностью открытой двери

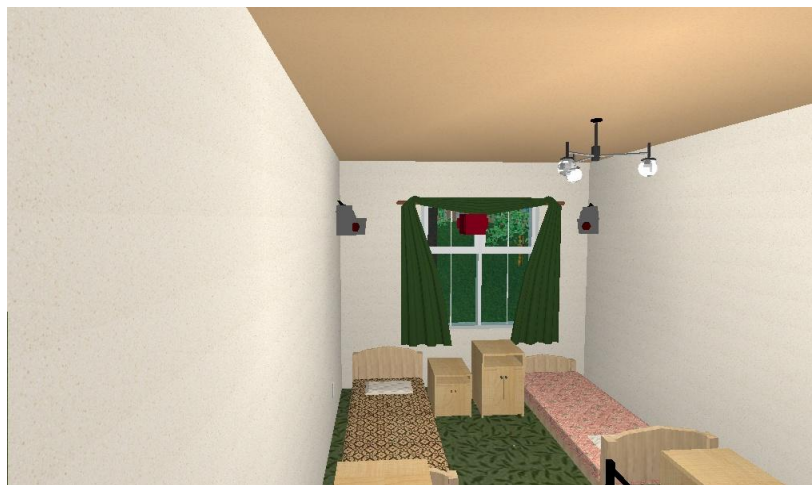


Рисунок 2.8 — Вид контролируемого помещения при установке устройства съема видовой информации на шкаф (приложение А, поз. 5)

Оценка угрозы:

— время необходимое для организации канала утечки информации (для установки оптических устройств 1 час);

— время необходимое для обнаружения канала утечки информации, для нахождения устройства — 1 день, т.к. устройство установлено за пределами КЗ;

— время для ликвидации канала утечки информации (для изъятия устройства) — 10 минут.

Оценка возможности организации: 5, т.к. требуются минимальные затраты средств, установка устройства не составляет труда.

Оценка привлекательности информации: 5, т.к. визуальная информация важна.

Оценка по степени опасности: 3.

3. ОЦЕНКА УРОЗ

С учетом проставленных оценок для показателей негативного воздействия и вероятностей реализации угроз для каждого канала утечки информации, рассчитаем общие показатели:

Коэффициент опасности канала утечки информации вычисляется по формуле [1]

$$k_{\text{опасности}} = \sum_{i=1}^n \frac{k_i}{5^n}, \quad (2)$$

Коэффициент опасности для визуально-оптического канала

$$k_{\text{оп1}} = \frac{3 \times 5 \times 5}{5^3} = 0,6.$$

Коэффициент опасности для акустического канала

$$k_{\text{оп2}} = \frac{4 \times 3 \times 4}{5^3} = 0,384 .$$

Коэффициент опасности информации виброакустического канала

$$k_{\text{оп3}} = \frac{3 \times 5 \times 4}{5^3} = 0,48 .$$

Коэффициент опасности информации для лазерного канала утечки информации:

$$k_{\text{оп4}} = \frac{4 \times 4 \times 3}{5^3} = 0,384 .$$

Каждый канал имеет определенную степень угрозы и характеризуется оценками, представленными в таблице 3.

Таблица 3 — Характеристики показателей негативного воздействия и реализации угрозы

Вид утечки информации	Показатель степени угрозы	Показатель вероятности реализации угрозы	Привлекательность информации	Коэффициент опасности
Визуально-оптический канал	3	5	5	0,6
Акустический канал	4	4	3	0,384
Виброакустический канал	3	4	4	0,48
Лазерный канал	3	4	4	0,384

Сводные данные по времени организации, нахождения и ликвидации каналов утечки информации представлены в таблице 4.

Таблица 4 — Характеристики показателей времени осуществления и обнаружения каналов угроз

Вид утечки информации	Время осуществления канала	Время обнаружения канала	Время ликвидации канала
Визуальнооптический канал	1 час	1 день	10 минут
Акустический канал	6 часов	30 минут	1 час
Виброакустический канал	1 часа	2 часа	10 минут
Лазерный канал	6 часов	30 минут	1 час

ЗАКЛЮЧЕНИЕ

Проанализировав все данные по каналам утечки информации, можно сделать вывод, что визуально-оптический канал является наиболее уязвимым каналом, поскольку показатели негативного воздействия и вероятности реализации угроз наиболее максимальные. А использование других каналов маловероятно вследствие их малой эффективности, трудоемкости и высокой опасности расшифровки.

Учитывая показатели коэффициента опасности, делаем заключение, что помещение уязвимо для попыток несанкционированного доступа к секретной информации, но вероятность реализации угроз мала, т.к. информация, циркулирующая в помещении, не представляет особой ценности для злоумышленников. Проведя анализ наиболее вероятных мест установки оборудования можно сделать вывод, что самым уязвимым местом в ОИ является восточное окно (приложение А, поз. 23).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Стандарт ISO:17799-00 (Стандарт Великобритании BS 7799-95 "Практические правила управления информационной безопасностью")
2. Парошин, А.А. Нормативно-правовые аспекты защиты информации: Учебное пособие. — Владивосток: Изд-во Дальневост. федер. ун-та, 2010. — 116 с.
3. Зайцев, А.П., Шелупанов, А.А. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. — М. : ООО «Издательство Машиностроение», 2009. — 508 с.
4. Гатчин, Ю.А., Климова Е.В. Основы информационной безопасности: Учебное пособие. — СПб: СПбГУ ИТМО, 2009. — 84 с.
5. Нестеров С.А. Информационная безопасность и защита информации: Учебное пособие. — СПб.: Изд-во Политехн. ун-та, 2009. — 126 с.
6. Сидорин Ю.С. Технические средства защиты информации: Учебное пособие. — СПб.: СПбГПУ, 2005. — 141 с.
7. Хореев, А. А. Защита информации от утечки по техническим каналам. Ч. 1. Технические каналы утечки информации : учебное пособие / А. А. Хореев. — М. : Гостехкомиссия России, 1998. — 320 с.
8. Бузов, Г. А. Защита от утечки информации по техническим каналам : учебное пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. — М. : Горячая линия — Телеком, 2005. — 416 с.
9. Хореев, А. А. Классификация и характеристика технических каналов утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи / А. А. Хореев // Специальная техника. — 1998. — № 2. — С. 41—46.
10. «Шпионские штучки» и устройства для защиты объектов и информации : справочное пособие. — СПб. : Лань, 1996. — 95 с.

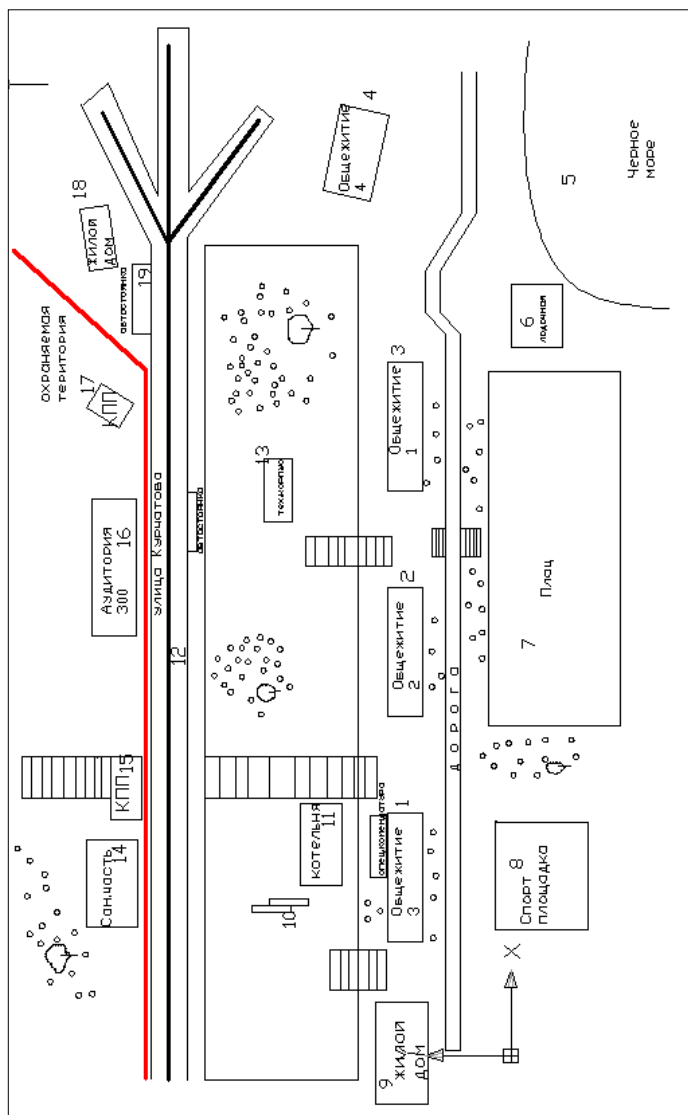
11. Лобашев, А. К. Современное состояние и тактические возможности применения индикаторов электромагнитных излучений / А. К. Лобашев, Л. С. Лосев // Специальная техника. — 2004. — № 6. — С. 36—45.

12. Бузов, Г. А. Современный взгляд на решение проблемы применения «легальных жучков» / Г. А. Бузов, А. К. Лобашев, Л. С. Лосев // Защита информации. Инсайд. — 2005. — № 2. — С. 52—53.

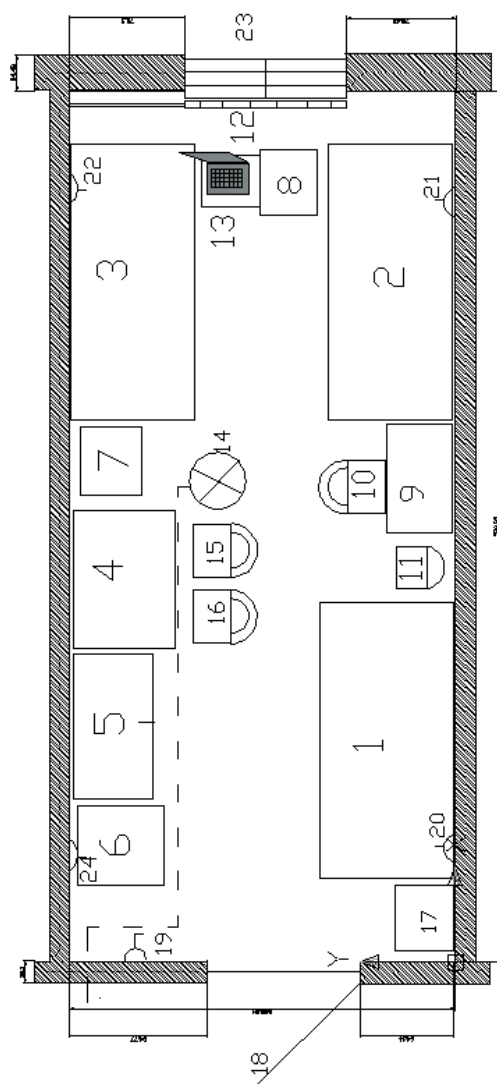
13. Бузов, Г. А. Концептуальные основы подготовки специалистов по информационной безопасности / Г. А. Бузов, А. К. Лобашев // Защита информации. Инсайд. — 2005. — № 6. — С. 62—65.

14. Лобашев, А. К. Дифференциация поисковых подходов при выявлении службами безопасности закладных устройств / А. К. Лобашев // Защита информации. Инсайд. — 2006. — № 5. — С. 26—32.

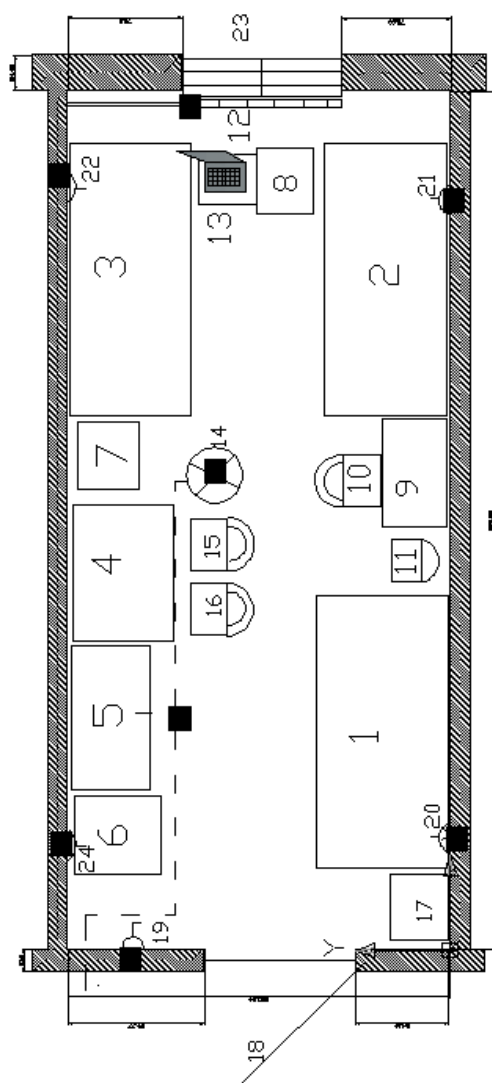
Приложение Г. СИТУАЦИОННЫЙ ПЛАН



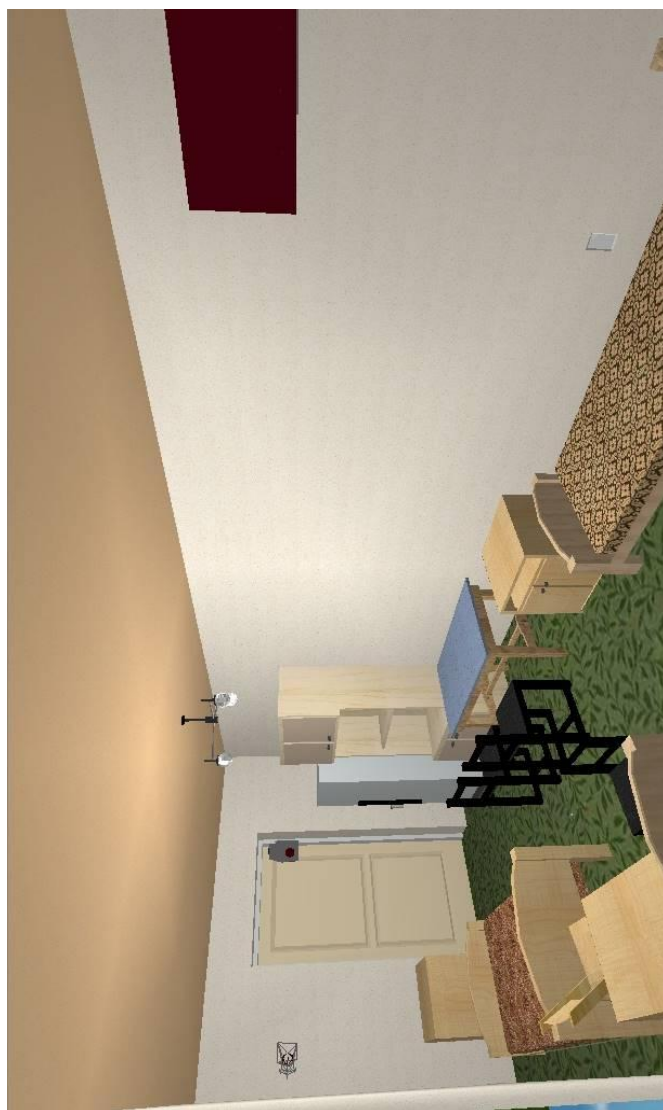
Приложение Д. ГЕНЕРАЛЬНЫЙ ПЛАН



Приложение Е. **АКУСТИЧЕСКИЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ**



Приложение Ж.
ПРОЕКТ КОМНАТЫ В 3D ФОРМАТЕ



Приложение И.

РАНЖИРОВАНИЕ ИСТОЧНИКОВ УГРОЗ

Все источники угроз имеют разную степень опасности $(K_{\text{оп}})_i$, которую можно количественно оценить, проведя их ранжирование. При этом, оценка степени опасности проводится по косвенным показателям. В качестве критериев сравнения (показателей) можно, к примеру, выбрать:

— **возможность возникновения источника $(K_1)_i$** — определяет степень доступности к защищаемому объекту (для антропогенных источников), удаленность от защищаемого объекта (для техногенных источников) или особенности обстановки (для случайных источников);

— **готовность источника $(K_2)_i$** — определяет степень квалификации и привлекательность совершения деяний со стороны источника угрозы (для антропогенных источников), или наличие необходимых условий (для техногенных и стихийных источников);

— **фатальность (опасность) $(K_3)_i$** — определяет степень неустранимости последствий реализации угрозы.

Каждый показатель оценивается экспертно-аналитическим методом по пятибалльной системе. Причем, единица соответствует самой минимальной степени влияния оцениваемого показателя на опасность использования источника, а пятерка — максимальной.

$(K_{\text{оп}})_i$ для отдельного источника можно определить, как отношение произведения вышеприведенных показателей к максимальному значению

$$(K_{\text{оп}})_i = \frac{K_1 \cdot K_2 \cdot K_3}{5^3}$$

Степень доступности к защищаемому объекту может быть классифицирована по следующей шкале:

— **высокая степень доступности (5)** — антропогенный источник угроз имеет полный доступ к техническим и программным средствам обработки защищаемой информации (характерно для внутренних антропогенных источников, наделенных максимальными правами доступа, например, представители служб безопасности информации, администраторы);

— **первая средняя степень доступности (4)** — антропогенный источник угроз имеет возможность опосредованного, не определенного функциональными обязанностями, (за счет побочных каналов утечки информации, использования возможности доступа к привилегированным рабочим местам) доступа к техническим и программным средствам обработки защищаемой информации (характерно для внутренних антропогенных источников);

— **вторая средняя степень доступности (3)** — антропогенный источник угроз имеет ограниченную возможность доступа к программным средствам в силу введенных ограничений в использовании технических средств, функциональных обязанностей или по роду своей деятельности (характерно для внутренних антропогенных источников с обычными правами доступа, например, пользователи, или внешних антропогенных источников, имеющих право доступа к средствам обработки и передачи защищаемой информации, например, хакеры, технический персонал поставщиков телематических услуг);

— **низкая степень доступности (2)** — антропогенный источник угроз имеет очень ограниченную возможность доступа к техническим средствам и программам, обрабатывающим защищаемую информацию (характерно для внешних антропогенных источников);

— **отсутствие доступности (1)** — антропогенный источник угроз не имеет доступа к техническим средствам и программам, обрабатывающих защищаемую информацию.

Примеры характеристик нескольких показателей

Степень удаленности от защищаемого объекта можно характеризовать следующими параметрами:

— **совпадающие объекты** — объекты защиты сами содержат источники техногенных угроз и их территориальное разделение невозможно;

— **близко расположенные объекты** — объекты защиты расположены в непосредственной близости от источников техногенных угроз, и любое проявление таких угроз может оказать существенное влияние на защищаемый объект;

— **средне удаленные объекты** — объекты защиты располагаются на удалении от источников техногенных угроз, на котором проявление влияния этих угроз может оказать не существенное влияние на объект защиты;

— **удаленно расположенные объекты** — объект защиты располагается на удалении от источника техногенных угроз, исключая возможность его прямого воздействия;

— **сильно удаленные объекты** — объект защиты располагается на значительном удалении от источников техногенных угроз, полностью исключая любые воздействия на защищаемый объект, в том числе и по вторичным проявлениям.

Особенности обстановки характеризуются расположением объектов защиты в различных природных, климатических, сейсмологических, гидрологических и других условиях. Особенности обстановки можно оценить по следующей шкале:

— **очень опасные условия** — объект защиты расположен в зоне действия природных катаклизмов;

— **опасные условия** — объект защиты расположен в зоне, в которой многолетние наблюдения показывают возможность проявления природных катаклизмов;

— **умеренно опасные условия** — объект защиты расположен в зоне в которой по проводимым наблюдениям на протяжении долгого периода отсутствуют проявления природных катаклизмов, но имеются предпосылки возникновения стихийных источников угроз на самом объекте;

— **слабо опасные условия** — объект защиты находится вне пределов зоны действия природных катаклизмов, однако на объекте имеются предпосылки возникновения стихийных источников угроз;

— **неопасные условия** — объект защиты находится вне пределов зоны действия природных катаклизмов и на объекте отсутствуют предпосылки возникновения стихийных источников угроз.

Квалификация антропогенных источников играет важную роль в определении их возможностей по совершению противоправных деяний. Классификация уровня квалификации по возможности (уровню) взаимодействия с защищаемой АС:

— **нулевой уровень** — определяется отсутствием возможности какого-либо использования программ;

— **первый уровень** — ограничивается возможностью запуска задач/программ из фиксированного набора, предназначенного для обработки защищаемой информации (уровень неквалифицированного пользователя);

— **второй уровень** — учитывает возможность создания и запуска пользователем собственных программ с

новыми функциями по обработке информации (уровень квалифицированного пользователя, программиста);

— **третий уровень** — определяется возможностью управления функционированием сетью, то есть воздействием на базовое программное обеспечение, ее состав и конфигурацию (уровень системного администратора);

— **четвертый уровень** — определяется всем объемом возможностей субъектов, осуществляющих проектирование и ремонт технических средств, вплоть до включения в состав сети собственных технических средств с новыми функциями по обработке информации (уровень разработчика и администратора).

Привлекательность совершения деяния со стороны источника угроз устанавливается следующим образом:

— **особо привлекательный уровень** — защищаемые информационные ресурсы содержат информацию, которая может нанести непоправимый урон и привести к краху организации, осуществляющей защиту;

— **привлекательный уровень** — защищаемые информационные ресурсы содержат информацию, которая может быть использована для получения выгоды в пользу источника угрозы или третьих лиц;

— **умеренно привлекательный уровень** — защищаемые информационные ресурсы, содержат информацию, разглашение которой может нанести ущерб отдельным личностям;

— **слабо привлекательный уровень** — защищаемые информационные ресурсы содержат информацию, которая при ее накоплении и обобщении в течение определенного периода может причинить ущерб организации, осуществляющей защиту;

— **не привлекательный уровень** — информация не представляет интерес для источника угрозы.

Необходимые условия готовности источника определяются исходя из возможности реализации той или иной угрозы в конкретных условиях расположения объекта. При этом предполагается:

— **угроза реализуема** — то есть условия благоприятны или могут быть благоприятны для реализации угрозы (например, активизация сейсмической активности);

— **угроза умеренно реализуема** — то есть условия благоприятны для реализации угрозы, однако долгосрочные наблюдения не предполагают возможности ее активизации в период существования и активной деятельности объекта защиты;

— **угроза слабо реализуема** — то есть существуют объективные причины на самом объекте или в его окружении, препятствующие реализации угрозы;

— **угроза не реализуема** — то есть отсутствуют предпосылки для реализации предполагаемого события.

Степень неустранимости последствий проявления угрозы (фатальность) определяется по следующей шкале:

— **неустранимые последствия** — результаты проявления угрозы могут привести к полному разрушению (уничтожению, потере) объекта защиты, как следствие к невосполнимым потерям и исключению возможности доступа к защищаемым информационным ресурсам;

— **практически неустранимые последствия** — результаты проявления угрозы могут привести к разрушению (уничтожению, потере) объекта и к значительным затратам (материальным, временным и пр.) на восстановление последствий, сопоставимых с затратами на создание нового объекта и существенному ограничению времени доступа к защищаемым ресурсам;

— **частично устранимые последствия** — результаты проявления угрозы могут привести к

частичному разрушению объекта защиты и, как следствие, к значительным затратам на восстановление, ограничению времени доступа к защищаемым ресурсам;

— **устранимые последствия** — результаты проявления угрозы могут привести к частичному разрушению (уничтожению, потере) объекта защиты, не требующих больших затрат на его восстановление и, практически не влияющих на ограничение времени доступа к защищаемым информационным ресурсам;

— **отсутствие последствий** — результаты проявления угрозы не могут повлиять на деятельность объекта защиты.

Результаты проведенного ранжирования относительно конкретного объекта защиты можно свести в таблицу, позволяющую определить наиболее опасные для данного объекта источники угроз безопасности информации.

При выборе допустимого уровня источника угроз предполагается, что источники угроз, имеющие коэффициент $(K_{оп})_i$ менее $(0,1—0,2)$ могут в дальнейшем не учитываться, как маловероятные.

Определение актуальных (наиболее опасных) угроз осуществляется на основе анализа расположения объектов защиты и структуры построения информационной системы, а также информационных ресурсов, подлежащих защите.

Определение актуальных угроз

При определении актуальных угроз, экспертно-аналитическим методом определяются объекты защиты, подверженные воздействию той или иной угрозы, характерные источники этих угроз и уязвимости, способствующие реализации угроз.

На основании анализа составляется матрица взаимосвязи источников угроз и уязвимостей из которой

определяются возможные последствия реализации угроз (атаки) и вычисляется коэффициент опасности этих атак как произведение коэффициентов опасности соответствующих угроз и источников угроз, определенных ранее. При этом предполагается, что атаки, имеющие коэффициент опасности менее 0,1 (предположение экспертов), в дальнейшем могут не рассматриваться из-за малой вероятности их совершения на рассматриваемом объекте.

Такая матрица составляется отдельно для каждой угрозы.

Таким образом, процедура, методика определения актуальных угроз выглядит следующим образом:

- определение множества угроз;
- для каждой угрозы определяются экспертно-аналитическим методом объекты защиты (данные, ПО, СВТ), подверженные действию той или иной угрозы;
- для объектов защиты определяются (если еще неизвестны) требования к защищенности;
- определяются и ранжируются характерные источники угроз. Отбрасываются те, коэффициент опасности которых меньше $a = 0.1—0.2$. При этом величина a зависит от уровня требований к защищенности;
- определяются и ранжируются уязвимости АС, характерные для данного вида угроз;
- составляется матрица взаимосвязи источников угроз и уязвимостей: строки — источник угроз, столбцы — уязвимости. Значения элементов — коэффициент опасности атаки (произведение коэффициента опасности источника на коэффициент опасности уязвимости). Угроза считается несущественной, если коэффициент опасности атаки $b < 0.1$;
- проведенный анализ можно уточнять, детализируя объекты защиты.

На основе сделанной ранее оценки ценности объектов защиты (и требований к степени их защиты), а также прогнозирования вероятности воздействия на компоненты АС (коэффициент опасности атак) можно определить объем потенциальных потерь при возможной реализации угроз.

Оценка рисков

На первом шаге оценивается негативное воздействие (показатель ценности ресурса) по заранее определенной шкале (скажем, от 1 до 5) для каждого ресурса, которому угрожает опасность (ряд b в таблице).

На втором — по той же шкале оценивается актуальность угрозы, т.е. вероятность ее реализации.

На третьем шаге вычисляется показатель риска. В простейшем варианте методики это делается путем умножения ($b \times c$). Однако необходимо помнить, что операция умножения определена для количественных шкал. Для ранговых (качественных) параметров, каковыми являются показатель негативного воздействия и вероятность реализации угрозы, показатель риска в случае, если $b = 1$, $c = 3$, совсем не обязательно будет эквивалентен $b = 3$, $c = 1$. Соответственно должна быть разработана методика оценки показателей рисков применительно к конкретной организации.

На четвертом шаге угрозы ранжируются по значениям их фактора риска.

В рассматриваемом примере для обозначения наименьшего негативного воздействия и наименьшей вероятности реализации выбран показатель 1.

Данная процедура позволяет сравнивать и ранжировать по приоритету угрозы с различными негативными воздействиями и вероятностями реализации.

Применение каких-либо инструментальных средств не является обязательным, однако позволяет уменьшить трудоемкость анализа рисков и выбора контрмер.

Таблица И.1 — Результаты расчета оценки рисков для объекта

Дескриптор угрозы	Угроза А	Угроза Б	Угроза В	Угроза Г	Угроза Д	Угроза Е
Показатель негативного воздействия ресурса	5	2	3	1	4	2
Вероятность реализации угрозы	2	4	5	3	1	4
Показатель риска	10	8	15	3	4	8
Ранг угрозы	2	3	1	5	4	3