МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

кафедра Автоматической электросвязи

«Допущен к защите»
Заведующий кафедрой АЭС
Чежимбаева К.С., к.т.н., доцент
(Ф.И.О., ученая степень, звание)
_____ «_____»_____**20__ г.**
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Реализация и исследование математической модели оценки ущерба конфиденциальной информации от угроз

Специальность 5В071900-Радиотехника, электроника и телекоммуникации

Выполнил (а) Сактаганов Ж.К. СТК-10-04
(Фамилия и инициалы) группа

Научный руководитель Акубова М.З., к.т.н., профессор
(Фамилия и инициалы, ученая степень, звание)

Консультанты:
по экономической части:
Бабич А.А., ст. преподаватель
(Фамилия и инициалы, ученая степень, звание)
_____ «29» мая 2014 г.
(подпись)

по безопасности жизнедеятельности:
Санатова Ш.С., к.т.н., доцент
(Фамилия и инициалы, ученая степень, звание)
_____ «23» мая 2014 г.
(подпись)

по применению вычислительной техники:
Туманбаева Ж.К., к.т.н., профессор
(Фамилия и инициалы, ученая степень, звание)
_____ «06» 06 2014 г.
(подпись)

Нормоконтролер: Абиров Д.А., ст. преподаватель
(Фамилия и инициалы, ученая степень, звание)
_____ «12» 06 2014 г.
(подпись)

Рецензент: Кубекова Б.С. к.т.н., проф.
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____20___г.
(подпись)

Алматы 2014 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет Радиотехники и связи
Специальность 5В071900 – Радиотехника, электроника и телекоммуникации
Кафедра Автоматической электросвязи

ЗАДАНИЕ

на выполнение дипломного проекта

Студент Сактаганов Касымхан Жикбаевич
(фамилия, имя, отчество)

Тема проекта Реализация и исследование математической модели оценки ущерба конфиденциальной информации от угроз

утверждена приказом ректора № ___ от «___» сентября 20___ г.
Срок сдачи законченной работы «___» _____ 20___ г.
Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта

1. Математическая модель оценки ущерба
2. $P_{обн}$: 0,1; 0,2; 0,3; 0,4; 0,5; 0,6; 0,7; 0,8; 0,9
3. $U_р$: 4737; 9474; 14211; 18948; 23685; 28422; 33159; 37896; 42633;
4. $P_{расп}$: 0,1; 0,2; 0,3; 0,4; 0,5; 0,6; 0,7; 0,8; 0,9;
результаты исследования

Перечень подлежащих разработке дипломного проекта вопросов или краткое содержание дипломного проекта:

1. Анализ задачи оценки ущерба конфиденциальной информации
2. Построение математической модели оценки ущерба от воздействия на конфиденциальную информацию внешних угроз
3. Реализация и исследование математической модели оценки ущерба конфиденциальной информации от внешних угроз
4. Безопасность и экологичность работы
5. Бизнес план

Перечень графического материала (с точным указанием обязательных чертежей)

1. ИТ - система
2. схема атаки „навязывание ложного маршрута
3. Программный пакет Wireshark
4. схема метода Монте-Карло
5. Графическая модель взаимосвязи состояния осведомленности соперника об объекте
6. Зависимость величины раскрытого потенциала от изменения тех. оснащения злоумышленника

Рекомендуемая основная литература

1. Белов, Е.Б. Основы информационной безопасности: уч пос. для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов - М.: горячая линия
2. Грушина, М.В Организация комплексной защиты информации: уч. пособие
3. Бузов, Г.А. Защита от утечки информации по техн-м каналам: уч. пособие
4. Гмурман, В.Е. Теория вероятностей и математическая статистика:
5. Романец, Ю.В. Защита информации в компьютерных сетях и системах: уч. пособие

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
Технико-экономич. расчет	Бабич А.А.	19.05 - 29.05	
Безопасность жизнед.	Санатова Т.С.	23.05.2014г	
Применение ВТ	Турумбаева К.Х	20.04-06.06	
Рецензент	Кудеков Б.Р.	18.04.2014г.	
Нормоконтроль	Мар Э.А	12.06.14	

Г Р А Ф И К
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1.	Основные виды угроз конфиденциальной информации и проведение их классификацию	26.04.2014г.	выполнено
2.	Изучение основных методов оценки ущерба	9.05.2014г.	выполнено
3	Определение внешних параметров модели оценки ущерба	14.05.2014г	выполнено
4.	Строение математической модели оценки ущерба на основе конфиденциальной информации	21.05.2014г	выполнено
5	расчет технико-экономической эффективности проекта	26.05.2014г	выполнено
6.	Рассмотрение безопасности и экономичности проекта	01.05.2014г	выполнено

Дата выдачи задания «____»_____20___ г.

Заведующий кафедрой _____ _____
(подпись) (Фамилия и инициалы)

Руководитель _____ _____
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ _____
(подпись) (Фамилия и инициалы)

Аңдатпа

Берілген дипломдық жобада ақпарат құпиялығына(конфеденциалдығына) қауіптен болған шығынды бағалаудың математикалық моделі зерттеліп жүргізілді.

Жұмыстың техникалық бөлімінде құпия ақпаратқа сыртқы қауіптің әсерінен болған шығынның математикалық моделі құрылған.

Дипломдық жұмыстың экономикалық бөлімінде жобаның бизнес жоспары құрылып, сондай-ақ, бұл жүйені қолданатындардың қорғану жүйесін ендіргеннен кейін алатын түсімінің есебі шығарылған. Жобаның өмір кауіпсіздігі бөлімінде, ауаны салқындату мен өндірістік жарықтандыру есебі берілген.

Аннотация

В данном дипломном проекте проводится исследование математической модели оценки ущерба конфиденциальной информации от угроз.

В технической части работы построена математическая модель ущерба от воздействия внешних угроз на конфиденциальную информацию.

В экономической части был составлен бизнес план проекта, а также рассчитаны доходы от реализации внедрения защитной системы и обслуживания пользователей данной системы. В разделе безопасности жизнедеятельности рассчитаны кондиционирование воздуха и производственное освещение.

Содержание

Введение

Каждый эпоха развития человечества характеризуется некоторыми присущими для него особенностями. Современный мир легко можно назвать информационным. Мы окружены богатством информацией различных типов и назначений, и не вся эта информация предназначена для доступа широкого круга пользователей.

В соответствии с режимом доступа информация подразделяется на информацию с доступом открытым и ограниченным. А информация с ограниченным доступом, в свою очередь, подразделяется на секретную и конфиденциальную. Конфиденциальная информация это - данные, который находится в собственности тех или иных физических или юридических лиц, передаются третьим лицам только по их желанию и на их условиях.

По содержанию конфиденциальная информация может быть производственного, профессионального, коммерческого, банковского и прочего характера.

Почти во всех областях человеческой жизни есть информация, который не предназначено для широкого ряда пользователей. Чтобы значительно снизить вероятность злоумышленного доступа к конфиденциальной информации, в настоящее время существует много методов. Они очень хорошо разработаны, чтобы обеспечить полную защиту данных, но на практике никакой метод не обеспечивает 100% защиту от любых вредоносных действий. Поэтому разработаны методы для оценки размера ущерба от утечки информации, оценку рисков утечки конфиденциальной информации, методы оценки вероятности рисков необходимы для конфиденциальная информация, и т.д. Все эти методы являются полным анализом проблемы информационной безопасности.

Значимость исследований в этой области является то, что метод, разработанный для определения убытков, может определить и описать всевозможные способы реализации угроз. В дополнение к вышесказанных методов, следует отметить что владельцу конфиденциальной информации экономически не выгодно тратить больше средств на ее защиту, чем стоимость самой информации.

Таким образом, объектом исследования является алгоритм моделирования для оценки ущерба, вероятно, вызванное несанкционированного доступа к конфиденциальной информации в нападавшего в примере автоматизированной доступа информационной системы.

Цель состоит в том, чтобы построить математическую модель для определения возможного ущерба, вызванного от несанкционированного доступа к конфиденциальной информации.

Из поставленных целей, были определены нижеперечисленные задачи:

– Рассмотреть основные виды угроз конфиденциальной информации и провести их классификацию;

– Изучить основные методы оценки ущерба;

– Определить внешние параметры модели оценки ущерба;

– Построить математическую модель оценки ущерба на основе проведенных исследований.

Необходимо также отметить, что разработка и исследование новых методов оценки ущерба от угроз конфиденциальной информации, а также применение существующих позволяет в значительной степени повышает уровень систем защиты.

Целью дипломной работы является разработка модели оценки ущерба конфиденциальной информации от внешних угроз. Для достижения поставленной задачи требуется проанализировать виды угроз конфиденциальной информации, проанализировать основные методы оценки ущерба, определить внешние параметры модели оценки ущерба конфиденциальной информации от внешних угроз и построить модель оценки ущерба конфиденциальной информации от внешних угроз.

Работа состоит из 5 глав.

В первой главе рассматриваются анализ и классификация угроз конфиденциальной информации, существующих методов оценки ущерба конфиденциальной информации от внешних угроз.

Во второй главе рассматривается построение математической модели оценки ущерба от воздействия на конфиденциальную информацию внешних угроз.

В третьей главе рассматривается алгоритм построения математической модели оценки ущерба конфиденциальной информации от внешних угроз, Реализация алгоритма построения математической модели оценки ущерба и анализ влияния входных параметров модели на величину ущерба.

В четвертой главе рассчитывается технико-экономическая эффективность проекта.

В пятой главе рассматривается безопасность и экологичность проекта.

В заключении даются краткие выводы, сделанные в результате работы.

1 Анализ задачи оценки ущерба конфиденциальной информации

1.1 Описание информационных технологий

Информационная технология - это совокупность методов, технических и программных средств, обеспечивающая реализацию процессов создания, сбора, обработки, накопления, хранения, поиска и распространения информации, а также регламентированный порядок применения информационных процессов. При рассмотрении проблемы безопасности информационных технологий необходимо исходить из того, что существуют две основные противоборствующие стороны – владелец ресурсов, требующих своей защиты, и злоумышленник, который имеет мотивы и возможность для незаконного использования ресурсов, что может привести к нанесению морального или материального ущерба владельцу ресурсов. Под ресурсом в широком смысле понимается все, что представляет ценность с точки зрения владельца ресурса и является объектом защиты. В узком смысле ресурс – это часть информационной системы. Рассмотрим такие виды ресурсов: оборудование (физические ресурсы); информационные ресурсы (все виды документации); программное обеспечение (утилиты, различные вспомогательные программы); сервис и поддерживающая инфраструктура (обслуживание телекоммуникационных средств и средств вычислительной техники, энергоснабжение и т.п.).

Злоумышленник выступает как источник угроз безопасности, при этом источником угроз может выступать не только физическое лицо, но аппаратное и программное обеспечение и т.п.

В дальнейшем под угрозой безопасности будим понимать совокупность условий, факторов, событий, действий и явлений, реализация которых может привести к нанесению ущерба владельцу ресурсов. Владелец ресурсов вынужден предпринимать меры, направленные на предотвращение или уменьшение степени этих опасностей. В качестве основных классов угроз рассматривают угрозы нарушения конфиденциальности, целостности и доступности. Для эффективного противодействия злоумышленнику, владелец ресурсов должен составить как можно более полный перечень угроз, которые могут быть реализованы в конкретных условиях с учетом имеющихся слабостей в системе, которые делают возможной реализацию угрозы. Процесс определения угроз, уязвимостей, возможного ущерба на основе заданной модели нарушителя называется анализом риска. Полученные результаты позволяют сформулировать задачи по обеспечению безопасности, а затем требования по обеспечению ИТ-безопасности [1]. Задача охраны - это задача постановки целей для противодействия выявленных угроз для безопасности и удовлетворения требований политики безопасности. Требования безопасности по существу включают ИТ функциональные требования безопасности и

требования к достаточности (гарантия). Функциональные требования безопасности определить набор функций безопасности, которые должны быть реализованы для решения проблемы безопасности. Для механизмы безопасности и решения, осуществлять функции безопасности, которые могут быть признаны фактически требует уверенность в правильности своего выбора и надежности. Такая уверенность достигается за счет представления и реализации требований к достаточности капитала.

Основными объектами требованиям безопасности являются produkuty ИТ-приложений и ИТ-систем. Под информационной технологии продукта относится к потребителю поставляется готовым к применению оборудования, программного обеспечения или аппаратного и программного обеспечения средств для обработки информации. Компьютерная система является системой логистики. Типичная система показана на рисунке 1.1. Включает в себя набор технических средств массовой информации и обработки информации (ИТ продукта); информации и других ресурсов; серверы и пользователей, связанные с организационной, технологической и другой цели, к реализации структурных принципов обработки информации.

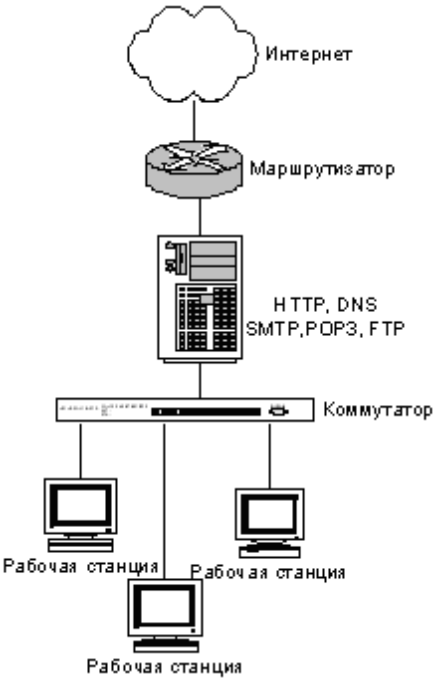


Рисунок 1.1 – ИТ-система

Главная цель безопасности информационных технологий заключается в обеспечении возможности любой организации решать свои функциональные задачи, задачи управление предприятием, технологическими процессами, подразделениями и т.д. путем построения ИТ-систем, которые исключают или минимизируют ИТ-риски организации, ее партнеров и потребителей.

1.2 Классификация угроз конфиденциальной информации

Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется атакой на информационную систему. Лица, преднамеренно реализующие угрозы, являются злоумышленниками.

Очень часто, угроза в связи с наличием уязвимостей в защите информационных систем, таких как неконтролируемого доступа к персональным компьютерам или нелицензионного программного обеспечения (к сожалению, даже лицензионное программное обеспечение не без уязвимостей).

История развития информационных систем показывает, что новые уязвимости постоянно растет. С той же регулярностью, но с небольшой задержкой, и есть средства.

В этом контексте более приемлемым является еще одним способом - форма проактивной защиты, является развитие механизмов защиты от возможных, вероятных и возможных угроз.

Некоторые угрозы не могут рассматриваться как результат целенаправленных действий пагубную природу. Есть угрозы, вызванные случайными ошибками или технологических явлений.

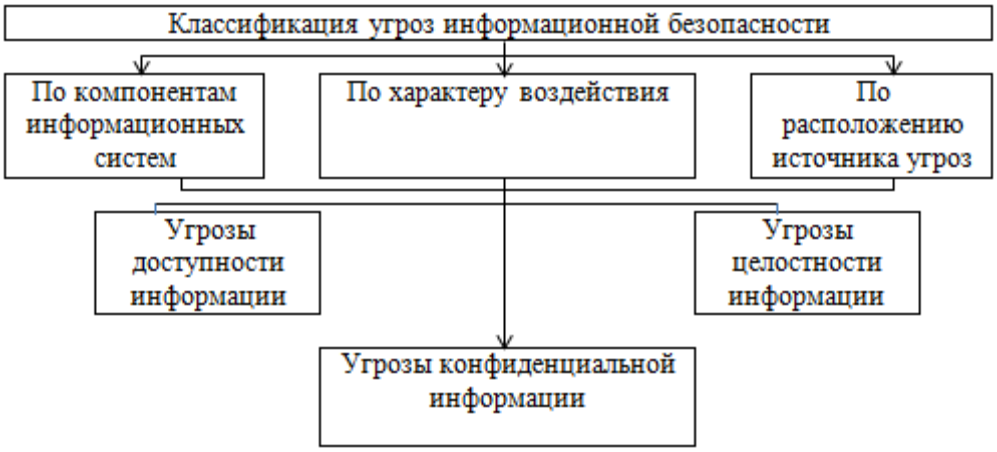


Рисунок 1.2 – Классификация угроз информационной безопасности

Знание потенциальных угроз безопасности, уязвимости и системы защиты, необходимо выбрать наиболее экономичные и эффективные средства для обеспечения безопасности.

Угрозы безопасности секретной информации по нескольким причинам:

- В компонентов информационной безопасности (доступность, целостность, конфиденциальность), против угроз, направленных в основном;
- Компоненты информационных систем, направленных угроз (данные, программы, оборудование, персонал);

- Характер воздействия (случайного или преднамеренного действия из природных или антропогенных);

- В места происхождения угроз (внутри системной информации считается или за пределами) [4].

Отправной точкой для анализа угроз информационной безопасности является определение компонент информационной безопасности, который может быть разделен в той или иной угрозы: конфиденциальность, целостность или доступность.

Угрозы классифицируются по источникам угроз месте, есть внутренние и внешние.

Внешние угрозы также исходить от субъектов, которые не являются частью пользователей и персонала системы, разработчиков системы, и не имеют прямого контакта с информационных систем и ресурсов.

Внутренние угрозы исходят от пользователей и систем обслуживания персонала, разработчиков систем, а также других учреждений, участвующих в процессах информации и имеют прямой контакт с информационных систем и ресурсов, утвержденных, и не иметь доступ к информации.

Источниками внешних угроз являются:

- В недобросовестные конкуренты;

- Милиция и преступные группировки;

- Частные лица и организации управления и административного персонала.

Источники внутренних угроз могут быть:

- Руководство компании;

- Личная;

- Технические средства производства и занятости.

Главной особенностью любой компьютерной сети является то, что ее компоненты распределены в пространстве. Связь между узлами сети физически реализуется посредством ПО и сетевых линий через механизм сообщений. Таким образом контролировать сообщений и данных, передаваемых между узлами в сети, пакеты передаются в виде обмена. Особенностью этого типа угрозы в том, что расположение злоумышленника изначально неизвестно.

Каждый угроза включает в себя некоторые повреждения - моральный или материальный, а также защиту и борьбу с угрозой намерена уменьшить его размер, в идеале - полностью реальная - или по крайней мере значительную часть. Но это не всегда возможно.

С учетом этой информации конфиденциальной угроза можно классифицировать следующим образом:

Степень ущерба, причиненного:

- Предел, после чего компания может стать банкротом;

- Значительное, но не приводит к банкротству;

- Свет, компания в течение некоторого времени и могут компенсировать друг друга;

Вероятность:

- Очень реальная угроза;
- Реальная угроза;
- Вряд ли угроза;

По соображениям появления:
- Стихийные бедствия;
- Умышленные действия;

По характеру повреждения:
- Материал;
- Моральный;

По характеру воздействия:
- Активный;
- Пассивный;

В связи с проектом:
- Внутренний;
- Внешний.

Поле воздействие информационных ресурсов и систем питания от угроз информационной безопасности можно разделить на внешние и внутренние с точки зрения их расположения в пределах или за пределами системы в ее проектирования и эксплуатации, а также возможных путей разместить нарушение безопасности приложения.

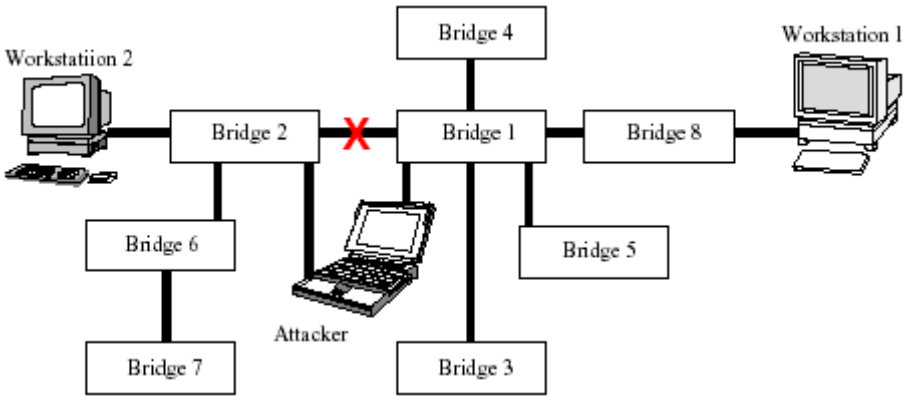


Рисунок 1.3 – схема атаки «навязывание ложного маршрута»

Попытка реализовать угроза называется атакой, и что делает попытку - злоумышленник. Нападающие называют потенциальные источники угрозы.

Очень часто, угроза в связи с наличием уязвимостей в защите информационных систем (таких, как возможность несанкционированного доступа к критической оборудования или ошибки программного обеспечения).

Период времени от момента, что становится возможным использовать слабое место, и пока разрыв не будет устранена, называемый окно опасности, связанной с слабости. В то время как есть окно опасности, возможность успешных атак на IP.

Если это ошибка в программном обеспечении, окно опасности "открывается" с появлением использования средств и исключает ошибку при

обновлении, чтобы исправить ее.

Опасность в окно самых уязвимых мест существует относительно долгое время (несколько дней, иногда недель -), потому что в это время следующие события должны произойти:

- Вы должны быть в курсе использования защиты космических средств;
- Соответствующие патчи будут опубликованы;
- Патчи должны быть установлены в защищенном интеллектуальной собственности.

Новые уязвимости и способы использовать их постоянно растет; Это означает, во-первых, что есть почти всегда окно опасности и, во-вторых, что отслеживание этих окон должно быть постоянным, а релиз и исправлений - как можно быстрее.

Некоторые угрозы не могут рассматриваться как результат ошибок или сбоев; которые существуют в связи с характером современных интегральных схем. Например, существует угроза перебоев в подаче электроэнергии или выходных параметров предельных значений, обусловленные зависимостью качества аппаратных питания IP. Будьте в курсе потенциальных угроз и уязвимостей на эти угрозы часто используются [5].

Необходимо выбрать наиболее экономически эффективным средством безопасности. Есть слишком много мифов в области информационных технологий, поэтому невежество в этом случае приводит к перерасходу средств и, что еще хуже, сконцентрировать ресурсы, где они не особенно необходимо, за счет наиболее уязвимых районах.

Понятие "угроза" в разных ситуациях часто относятся по-разному. Например, чтобы открыть организация подчеркнула угроз конфиденциальности, просто не может существовать - вся информация считается общественной информации; Однако, в большинстве случаев, незаконный доступ является серьезной опасностью. Другими словами, угрозы, как и все остальное в IB, зависят от интересов субъекта отношений информации (и какой вред неприемлемо для них).

Период времени от момента, что становится возможным использовать слабое место, и пока разрыв не будет устранена, называемый окно опасности, связанной с слабости. В то время как есть окно опасности, возможность успешных атак на IP. Очень часто, угроза в связи с наличием уязвимостей в области информационной безопасности.

1.3 Анализ потенциальных угроз конфиденциальной информации

Конфиденциальная информация - информация, которая не является государственной тайной, доступ к которой ограничен в соответствии с законодательством Российской Федерации.

Конфиденциальная информация, в свою очередь, включает в себя множество видов тайн, которые могут быть сведены к шести основных типов:

- Сведения о персоналиях;
- Тайна следствия и судопроизводства;
- Внутри тайны;
- Профессиональная тайна;
- Коммерческая тайна;
- Тайна изобретения, полезной модели и промышленного образца.

Под угрозы или опасности, потеря информации относится к одному или сложной, реального или потенциального, активного или пассивного проявления неблагоприятных особенностей внутренних или внешних угроз, чтобы создать критическую ситуацию, события оказать дестабилизирующее влияние на охраняемой информации, документов и баз данных.

Обобщенная схема потенциальных угроз конфиденциальной информации определяется параметром MΣ, характеризующего много угроз конфиденциальной информации, а также параметров M1, M2, ..., Mn - некоторые угрозы конфиденциальной информации. [6]

Риск любой угрозы дестабилизирующих эффектов (открытые и Ограниченный) информационные ресурсы создают стихийные бедствия, чрезвычайных ситуаций, аварий, техническое оборудование и коммуникационные линии и другие объективные обстоятельства, а также заинтересованы и незаинтересованным в случае угрозы к лицу. К угрозам, исходящим от этих лиц относятся: несанкционированное уничтожение документов, ускорение исчезновения (старения) текста или изображений, замены или удаления документов, фальсификации текста или его частей, и т.д.

Для информационных ресурсов ограниченного круга угроз, связанных с потерей информации (раскрытие информации, утечки) или потерю поддержки гораздо шире в результате того, что эти документы имеют больший интерес со стороны различных видов злоумышленников.

Под нападающим является лицо, действующее в интересах конкурента или противника в личных корыстных интересах (агенты иностранных разведок, промышленного и экономического шпионажа, криминальных организаций, отдельных преступников, тех, кто сотрудничает с атакующим, душевнобольных и т.д.).

- В отличие от обмена потери информации влечет за собой незаконное пересечение конфиденциальной информации и документов к предмету, который не имеет право владения и использовать их в своих целях.
- Основной угрозой для безопасности информационных ресурсов,

ограниченного распространения несанкционированного (незаконного, несанкционированного) доступа к атакующему или неуполномоченным лицом к документированной информации и в результате - овладение информации и ее использования незаконных или совершающих другие дестабилизирующих действий .

- Несанкционированное человек определяется как любое лицо, которое не имеет прямого отношения к компании (сотрудники из других организационных структур, муниципальных работников, очень осторожно, прохожих, посетителей фирм), а также сотрудников компании, не имея право доступа к некоторые помещения к определенному документу, информационной базы. Каждый из этих людей может быть более или его партнер, агент, но это не может быть он.
- Цели и результаты несанкционированного доступа может быть не только овладение ценной информации и их использование, но их изменение, изменение, уничтожение, фальсификация, замена и т.д.
- Необходимое условие для успешной реализации несанкционированного доступа к информационным ресурсам ограничен интерес к ним со стороны конкурентов, некоторые лица, услуг и организаций. При отсутствии такой информации, нет никакой угрозы интерес, даже если предпосылки, чтобы ознакомиться с его аутсайдером. Главный виновник несанкционированного доступа к информационным ресурсам, как правило, сотрудники, которые работают с документами, информацией и базами данных. При этом надо иметь в виду, что потеря информации в большинстве случаев не является результатом умышленных действий злоумышленника и халатности и безответственности на сотрудников. Следовательно, потеря информационных ресурсов ограниченного доступа может произойти, когда:

– наличии интереса конкурента, учреждений, фирм или лиц к конкретной информации;

– возникновении риска угрозы, организованной злоумышленником, или при случайно сложившихся обстоятельствах;

– наличии условий, позволяющих злоумышленнику осуществить необходимые действия и овладеть информацией.

Эти условия могут включать:

– отсутствие системной аналитической и контрольной работы по выявлению и изучению угроз, каналов и степени риска нарушений безопасности информационных ресурсов;

– неэффективную систему защиты информации или отсутствие этой системы, что образует высокую степень уязвимости информации;

– непрофессионально организованную технологию обработки и хранения конфиденциальных документов;

– неупорядоченный подбор персонала и текучесть кадров, сложный психологический климат в коллективе;

– отсутствие системы обучения сотрудников правилам защиты информации ограниченного доступа;

– отсутствие контроля со стороны руководства фирмы за соблюдением персоналом требований нормативных документов по работе с информационными ресурсами ограниченного доступа;

– бесконтрольное посещение помещений фирмы посторонними лицами.

Рассмотрение наиболее распространенных угроз, от которых страдает современный информационной системы дает представление о возможных угрозах, а также уязвимости, что эти угрозы, как правило, эксплуатируются, необходимо для того, чтобы выбрать наиболее экономически эффективным средством защиты.

Установка возможные угрозы безопасности проводится с целью определения полный список требований к системам безопасности. Список угроз, оценить вероятность их реализации, а также модель нарушителя обеспечивает основу для анализа рисков угроз и формулирование требований к системе защиты автоматизированной системы (АС). Кроме выявления возможных угроз следует проводить на основе их анализа классификаций [8].

1.4 Модель угроз

Свойства информации:

– конфиденциальность – свойство информации, которое заключается в том, что информация не может быть получена неавторизованным пользователем и/или процессом;

– доступность – свойство ресурса системы, которое заключается в том, что пользователь и/или процесс, которые имеют соответствующие полномочия, могут использовать ресурс соответственно правилам, установленных политикой безопасности, не ожидая дольше заданного (малого) промежутка времени, то есть когда он находится в виде, необходимом пользователю, в месте, необходимом пользователю, и в то время, когда он ему необходим;

– целостность - свойство информации, которое заключается в том, что информация не может быть модифицирована неавторизованным пользователем и/или процессом;

– аутентичность – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией, но уже автора сообщения;

– наблюдаемость – свойство ресурса, системы, которое позволяет фиксировать деятельность пользователей и процессов, использование пассивных объектов, а так же однозначно устанавливать идентификаторы причастных к некоторым событиям пользователей и процессов с целью предупреждения нарушений политики безопасности и/или обеспечить

ответственность за некоторые действия.

В результате анализе задания были выявлены следующие угрозы:

– нарушение конфиденциальности;
– нарушение целостности;
– нарушение доступности;
– нарушение аутентичности;
– нарушение наблюдаемости.
– хищение информации;
– незаконное копирование и распространение;
– утрата информации.

Данные угрозы реализуются следующим образом:

– перехват данных в сети (sniffer);
– выявление логина и пароли сети;
– кража информации, хранящейся на сервере;
– кража информации, хранящейся на компьютере-клиенте;
– получение информации о конфигурации сети модификация информации;
– отрицание подлинности;
– навязывание ложной информации.
– изменение потока сообщений на пути их передачи.
– получение прав root злоумышленником;
– Моделирование атак сети с помощью wireshark.

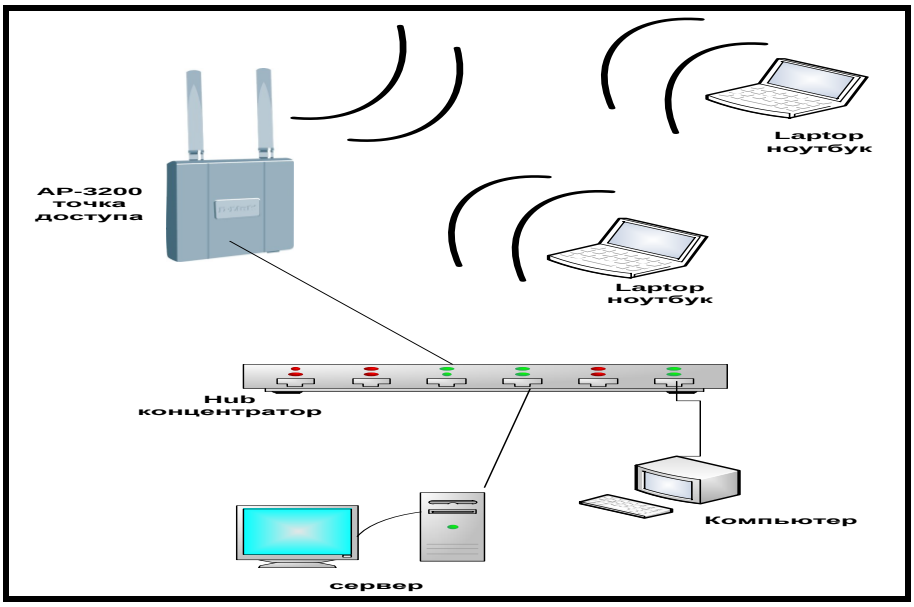


Рисунок 1.4 – схема проведения атаки на wireshark

1.5 Методы атак сети на основе программы Wireshark

«Wireshark» представляет собой мощный инструмент для моделирования атак на сети и обеспечивает возможности моделирования, визуализации, создания, оценки, а также совместной работы, которые поднимает качество квалификации преподавания и изучения сложных технологических концепций сетевых инструментов и программирования.

Для анализа и исследования безопасности сети с широкополосным Выберите инструмент для анализа и исследования таких сетей, где сеть от хакеров атаки могут быть сделаны на сервере, и где производительность требуется от сервера будет завышена, то есть будут более приемлемыми в Конструкция телекоммуникационных сетей. Рассмотрим один из этих программных средств, которые обеспечивают анализ любого сетевого трафика - "анализатор протокола Wireshark»

Пакет программного обеспечения «Wireshark» позволяет создавать сети с практически неограниченного числа устройств, практика, обнаружения, в сети контекстной рекламы трафика. Основываясь на окружающую среду обучения моделирования, Wireshark помогает пользователям развивать навыки, такие как принятие решений, творческого и критического мышления и решения проблем, а также для изучения движения сложных технических концепций сетевых систем. Polzovateli иметь возможность создавать, настраивать и изучить состояние транспортных сетей с использованием «Wireshark», объясняя концепцию сетей и технологий, основанных на различных технических средств.

Главное окно Wireshark делится на три панели. Размеры каждой из панелей могут быть изменены с помощью маркера в нижней правой части соответствующей панели.

На верхней панели из Wireshark содержит список пакетов. По умолчанию, список отображается 6 колонок - количество пакетов в списке собранной, временных меток, адреса и номера портов источника и назначения, протокол, а также краткое описание пакета.

Мы можем изменить набор отображаемых столбцов, используя страницу Столбцы диалоге настроек, чтобы активировать диалоговое окно, вы можете использовать команду меню Edit: Параметры или нажмите кнопку на панели инструментов Wireshark.

Нажав на поле с именем столбца в верхней части списка пакетов, мы можем определить сортировку пакетов содержимое этой колонке. Re кнопкой мыши на этом поле, чтобы изменить порядок сортировки.

В адрес полях отображается информация после максимального уровня. Например, обучение Ethernet, IP пакеты, содержащие адрес будут перечислены IP, но, если тип передаваемых кадров в протоколе, неизвестно, поле будет содержать MAC-адрес.

Правая кнопка мыши вызывает меню всплывающее для списка пакетов.

Средняя кнопка мыши может использоваться, чтобы отметить пакеты в

списке.

Ближний панель содержит дерево Wireshark протокол, выбранный из списка в верхней панели пакета. Дерево отображает каждое поле и его значение для названий всех стека протоколов. Структура каждой ветви дерева можно развернуть или свернуть, нажав кнопку мыши на площади в начале линии, соответствующей протокол. Правая кнопка мыши вызывает меню всплывающее для протокола дерева.

Нижняя панель окна содержит дамп списка пакетов в шестнадцатеричном и ASCII-формате. Выбранный в поле протокола дерево подсвечивается соответствующей области свалку правой кнопкой мыши активизирует всплывающее меню для панели свалку.

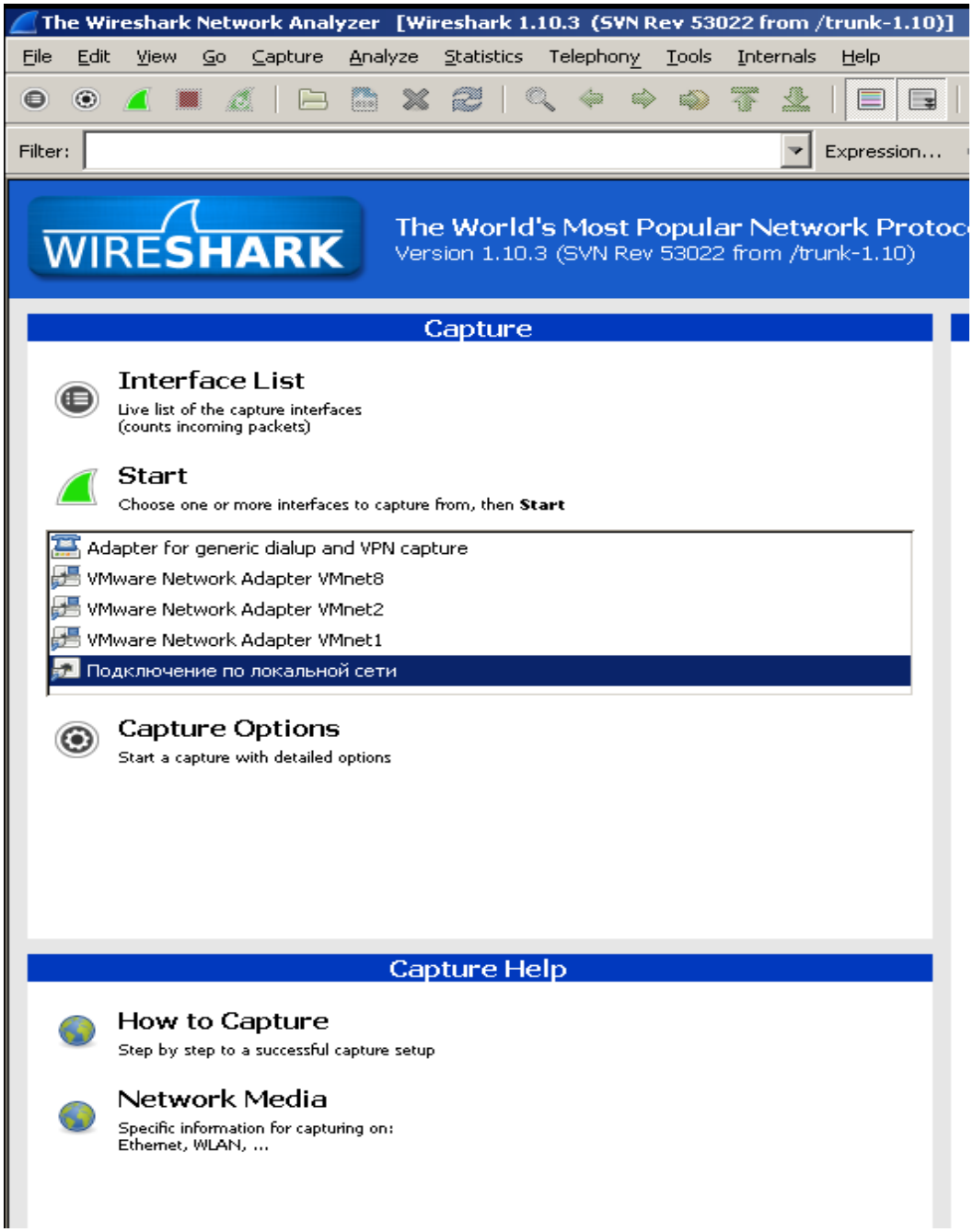


Рисунок 1.5 - главная панель Wireshark

Программный продукт «Wireshark» представляет собой программу для изучения трафика сетей любой сложности, а также позволяет изучать состояние безопасности сети технических средств и различных видов атак, сделанных хакерами. Создание сетей различных конфигураций, с помощью «Wireshark» может защитить при тестировании различных технических средств для создания объема пинги и изучить пути их прохождения. Кроме того, на основе анализа параметров могут быть выбраны технические средства информации. Использование «Wireshark», предназначены для защиты инструментов технического качества сетей. Wireshark работает с подавляющим большинством известных протоколов имеет четкую и логическую графический пользовательский интерфейс, основанный на GTK + и мощной системой фильтров. Кросс-платформенная, работает в ОС, таких как Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, и, конечно, Windows. Под лицензией GNU GPL.

1.6 Разработка схемы атаки на программе Wireshark

Чаще всего беспроводные точки доступа используются для предоставления доступа мобильным устройствам (ноутбуки, принтеры и т.д.) к стационарной локальной сети. Также беспроводные точки доступа часто используются для создания так называемых «горячих точек» — областей, в пределах которых клиенту предоставляется, как правило, бесплатный доступ к сети Интернет. Обычно такие точки находятся в библиотеках, аэропортах, уличных кафе крупных городов. В последнее время наблюдается повышение интереса к беспроводным точкам доступа при создании домашних сетей. Для создания такой сети в пределах одной квартиры достаточно одной точки доступа. Возможно, этого будет достаточно для включения в сеть и соседей прилегающих квартир. Для включения в сеть квартиры через одну, определенно, потребуется ещё одна точка доступа, которая будет служить ретранслятором сигнала, ослабевшего вследствие прохождения через несущую стену.

Для установки «точки доступа» требуется объединить компьютеры в беспроводную сеть и соединить этот сегмент сети с проводным. При использовании точки доступа мы имеем выделенное сетевое устройство, работа которого не зависит ни от загруженности других ПК, ни от их конфигурации, что является несомненным плюсом.

Для выполнения этой работы разработаем схему, приведенную на рисунке 1.6.1, где для его сборки необходимо иметь точку доступа, ноутбук, где установлена операционная система Windows 7 (или Windows XP имеющий беспроводный доступ).

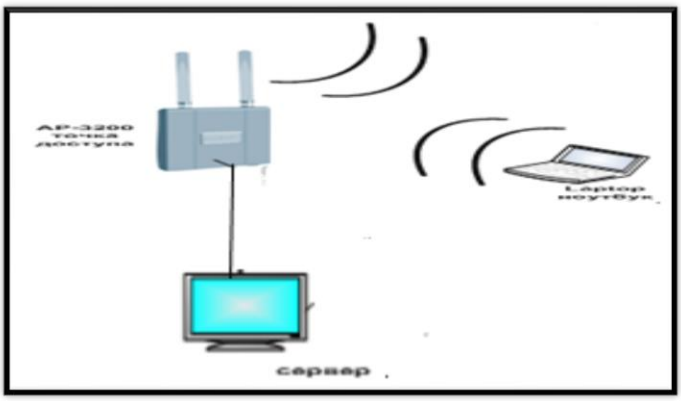
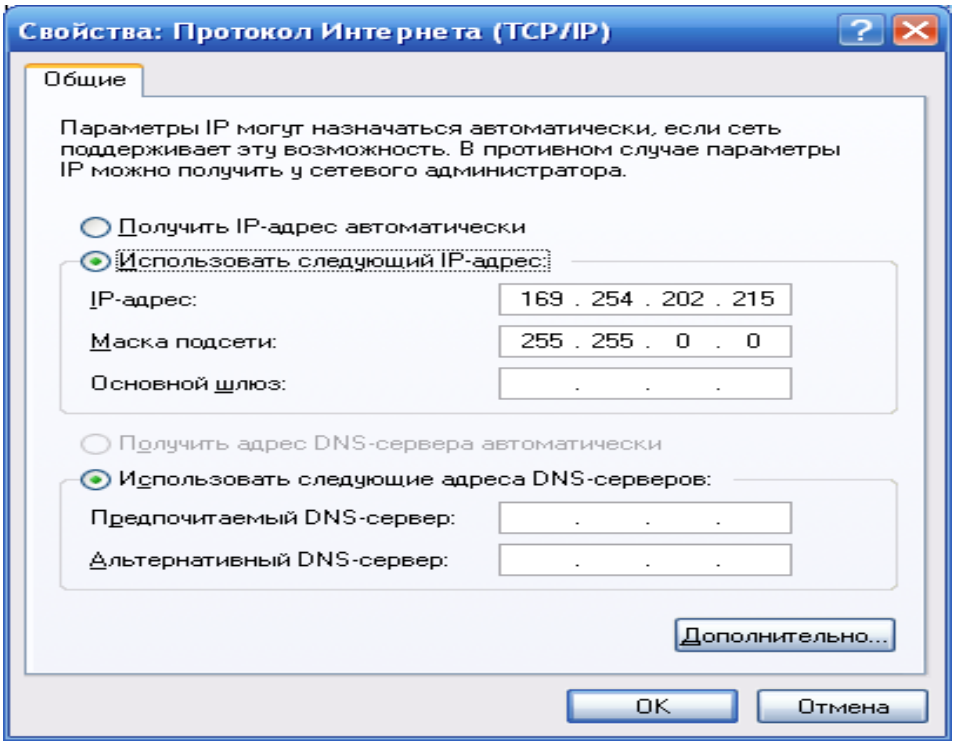


Рисунок 1.6.1 - Схема проведения эксперимента

Для проведения эксперимента:

- Соединяем точку доступа Интернета компьютера с кабелем с точкой доступа, определяем IP- адрес как показано на рисунке 1.6.2.



1.6.2 - Определение IP- адреса компьютера

- Устанавливаем программу ftpserv-110 на том же и прописываем нового пользователя, как показано на рисунке 1.6.3.

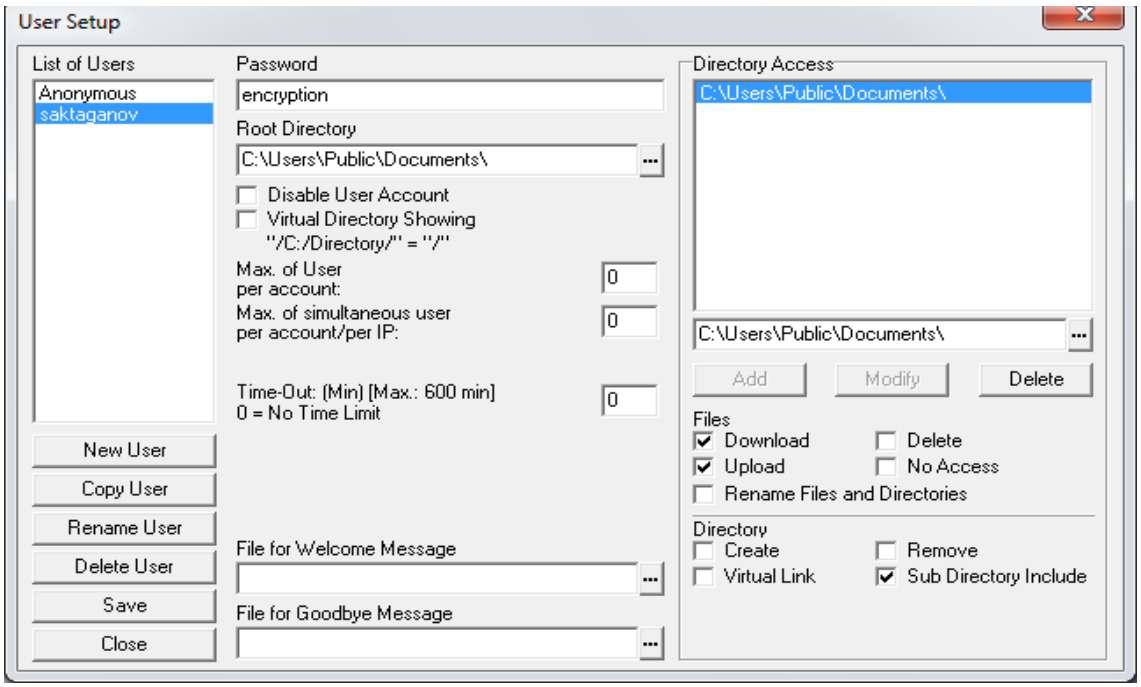


Рисунок 1.6.3 - Прописка нового пользователя

- Определяем IP- адрес клиента или компьютера имеющего беспроводный доступ. Для успешного проведения эксперимента необходимо иметь IP- адрес установленный в одной сети т.е, как показано на рисунке 1.6.4.

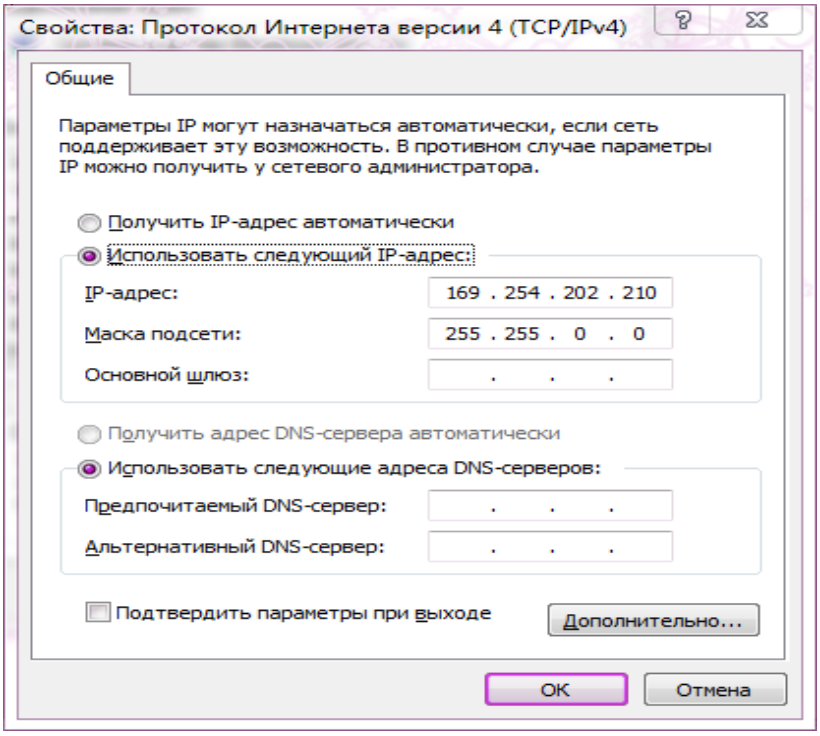


Рисунок 1.6.4 - IP- адрес клиента имеющего беспроводную точку доступа

- У клиента, имеющего беспроводное устройство установить программу FileZilla. Как показано на рисунке 1.6.5.

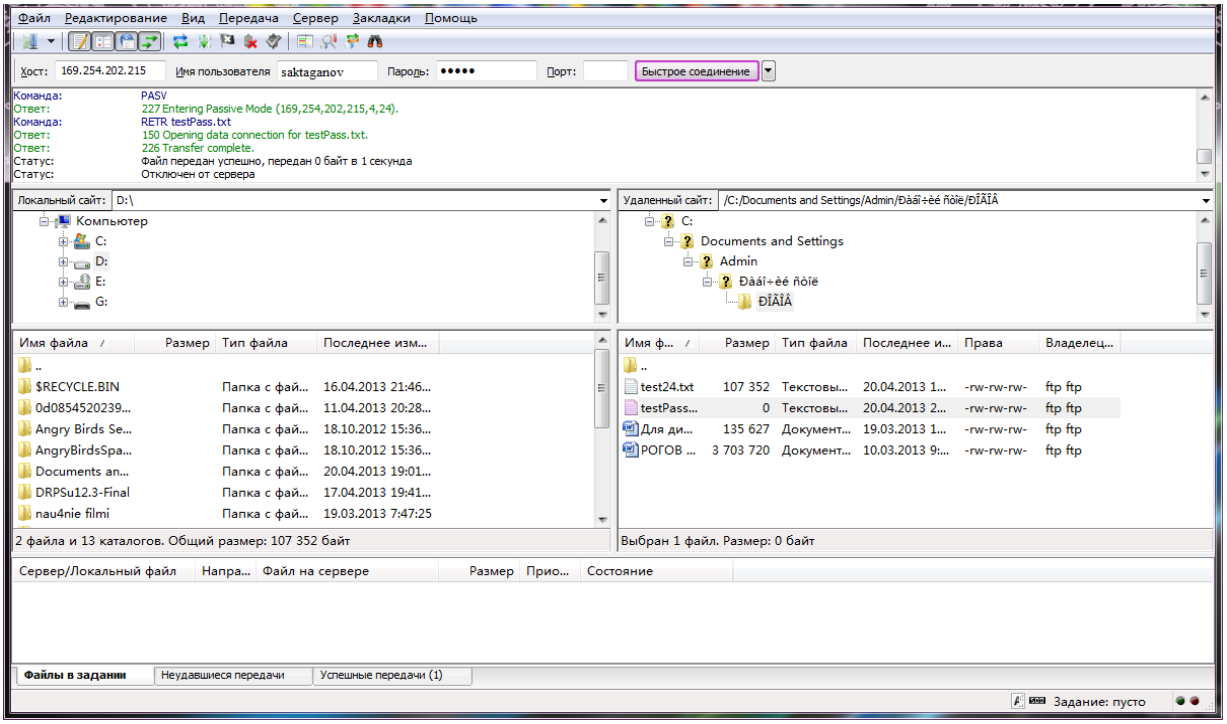


Рисунок 1.6.5 - Установка программы клиента FileZilla

- Для настройки клиентской программы для посылки запроса серверу набираем на программе данные пользователя как показано на рисунке 1.6.6.

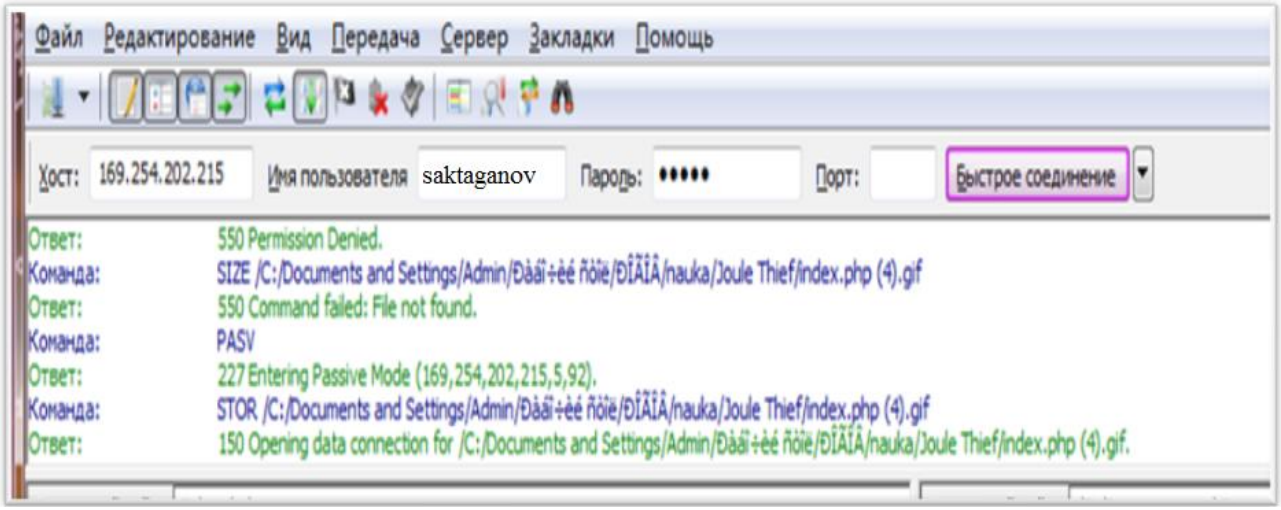


Рисунок 1.6.6 - Организация запроса к серверу

- И так можно прочитать обмен информацией между сервером и клиентом и далее в момент обращения клиента к серверу даны логин и далее пароль сервера рисунок 1.6.7, 1.6.8.

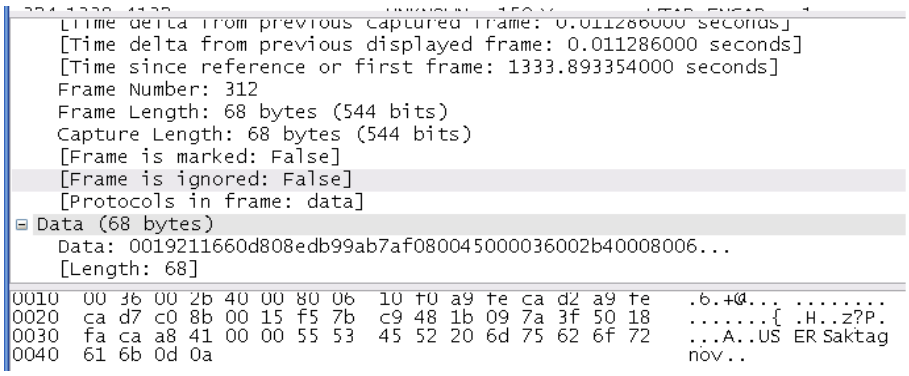


Рисунок 1.6.7 - Пассивная атака с определением логина сервера

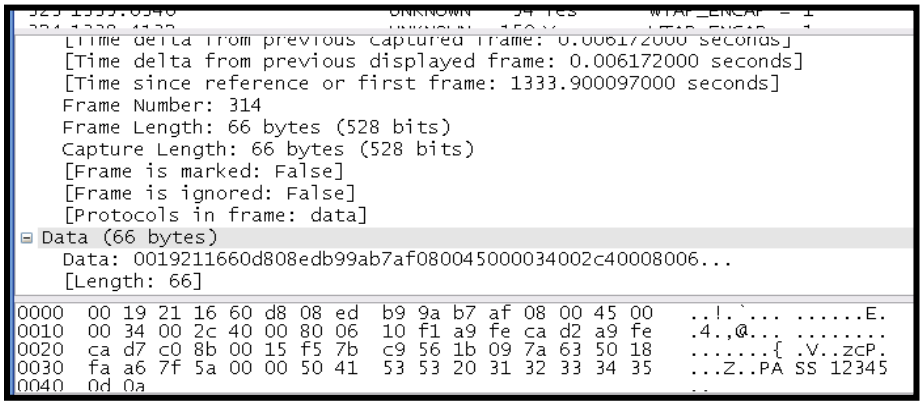


Рисунок 1.6.8. Определение пароля сервера при пассивной атаке

1.7 Анализ существующих методов оценки ущерба

В настоящее время, наряду с увеличением сложности и надежности методов защиты информации, улучшение методов несанкционированного доступа к конфиденциальной информации. Результат применяется к определенной экономической ущерб организации, которая в некоторых случаях может привести к серьезным последствиям. Для того чтобы определить заранее возможный ущерб, используют различные методы анализа. Среди них можно выделить следующие: естественный эксперимент, ЛИХ, методы математического моделирования и экспертных методов

Естественный эксперимент. Поле эксперимент, используемые в исследовании, как правило, внешних угроз, что приводит к значительным уровнем риска. Метод заключается в создании полной копии реального объекта защиты, а также все его отношений (внутренних и внешних) с другими объектами системы. После завершения подготовительного этапа полученной модели начинается моделирование различных вредоносных действий по осуществлению несанкционированного доступа к объекту охраны. Все

результаты моделирования документируются и подвергали статистическому анализу, на основе которой появляются практические рекомендации по обеспечению целостности информационной безопасности. Преимущество этого метода является высокая точность экспериментальных результатов, а также возможность в режиме реального времени и реальных систем для исследования задачи. Недостатком является сложность и высокая стоимость экспериментальных исследований, как это требуется для реализации на практике несколько десятков одинаковых экспериментов. Таким образом, применение этого метода весьма проблематично.

ЛИХ. ЛИХ не имеет недостатков натурных экспериментальных исследований. Этот метод устраняет необходимость создавать полную копию реального объекта. Суть метода состоит в замене некоторых частях реальной системы в определенной степени приближенных объектов. Это обычная практика при использовании этого метода заменяет только самые сложные реального объекта частей. Это снижает стоимость экспериментальных исследований и моделирования сложность уменьшается, но в результате точность и надежность данных также уменьшается пропорционально предположений, принятых при создании копии системы. Другим недостатком этого метода можно считать сходство отказ решение проблемы системного человек-машина реальной системе, в результате чего объективность и достоверность результатов уменьшается по сравнению с натурного эксперимента [8].

Методы математического моделирования. Математические методы моделирования являются одними из наиболее распространенных в моделирования и анализа ущерба, причиненного несанкционированного доступа к конфиденциальной информации.

По математического моделирования мы понимаем процесс установления соответствия с этим реальный объект математического объекта, называемого математической моделью и анализ этой модели, что позволяет получить характеристики реального объекта в стадии рассмотрения. Вид математической модели зависит от природы реального объекта, а объект исследования Задачи и требуемой надежности и точности решения этой проблемы. Любая математическая модель, как и любая другая, описывает реальный объект с определенной степенью приближения к действительности. Математическое моделирование для изучения свойств систем функционирования можно разделить на аналитической, моделирования и комбинированные.

Для аналитического моделирования характеризуется тем, что процессы функционирования элементов системы записываются в виде функциональных соотношений (алгебраических, интегро, конечной разности и т.п.) или логических условий. Аналитическая модель может быть проверена с помощью следующих методов:

–Аналитический при поиске, чтобы получить общий вид явных зависимостей для требуемых характеристик;

–численное когда, не в силах решить уравнения в целом, как правило,

получают численные результаты для конкретного исходных данных;

–Качественный когда без явных решений, мы можем найти некоторые свойства решения (например, для оценки устойчивости решения).

Наиболее полное исследование функционирования системы может осуществляться, если известные явные зависимости, связывающие желаемые характеристики от начальных условий, параметров и переменных системы С. Тем не менее, эти зависимости могут быть получены только для относительно простых систем. С их усложнением исследования систем аналитический метод наталкивается на значительные трудности, которые часто непреодолимыми. Так, желая использовать аналитический метод, в данном случае идти к существенному упрощению исходной модели, чтобы иметь возможность изучить хотя бы основные свойства системы. Такое исследование на упрощенной модели аналитического метода позволяет получить ориентировочные результаты, чтобы определить более точные оценки другими методами. Численный метод позволяет исследовать по сравнению с аналитическим методом более широкий класс систем, но решения являются частными. Численный метод особенно эффективен при использовании компьютера.

В некоторых случаях система может удовлетворить исследования и выводы, которые можно сделать с помощью качественного метода анализа математической модели. Эти качественные методы широко используются, например, в теории управления для оценки эффективности различных систем управления.

В алгоритме имитационного моделирования реализует модель воспроизводит процесс функционирования системы S в момент, моделируемые элементарные явления, составляющие процесс, с сохранением их логической структуры и последовательности течения времени, что позволяет исходные данные для получения информации о процесс утверждает, в определенное время, что позволяет оценить производительность системы S.

Основным преимуществом моделирования по сравнению с аналитических решений является возможность более сложных задач. Имитационные модели обеспечивают простой способ, чтобы принять во внимание такие факторы, как наличие дискретных и непрерывных элементов, нелинейные характеристики элементов системы, многочисленные случайные эффекты и т.д., которые часто создают трудности в аналитических исследований. В настоящее время моделирование - наиболее эффективный метод для изучения больших систем, и часто единственным практическим способом имеющейся информации о поведении системы, особенно на этапе ее проектирования.

Когда результаты, полученные при воспроизведении на имитационной модели функционирования системы S, являются реализациями случайных величин и функций, то найти характеристики процесса требуется свой повторный воспроизведение с последующей статистической обработки информации и необходимости в качестве метода компьютере Реализация

имитационных моделей использовать статистический метод моделирования. Был первоначально разработан метод Монте-Карло, который является численный метод, который был использован для моделирования случайных величин и функций, вероятностных характеристик которых совпадает с решением аналитических задач (эта процедура называется методом Монте-Карло) [9].

Рисунок 1.5 – схема метода Монте-Карло

Метод моделирования позволяет решать задачи анализа больших систем S, в том числе задач оценки: варианты структуры системы, эффективности различных алгоритмов управления системой, влияния изменения различных параметров системы. Имитационное моделирование может быть заложен в основу структурного, алгоритмического и параметрического синтеза больших систем, когда вы хотите создать систему с заданными характеристиками при определенных ограничениях, которая является оптимальной для некоторых критериев оценки эффективности.

При решении задач систем синтеза машин на основе их моделирования в дополнение к разработке алгоритмов моделирования для анализа фиксированной системы также должна разработать алгоритмы для нахождения оптимального варианта системы. Следующая в методологии компьютерного моделирования мы выделяем два основных раздела: статики и динамики - которые основное содержание соответственно вопросы анализа и систем синтеза данного алгоритма моделирования.

Комбинированное (аналитическое и имитационное моделирование) моделирование в анализе и систем синтеза позволяет сочетать преимущества аналитической и моделирования. При построении объединенные модели выполняется операция предварительной процесс разложения объекта на

составные суб-процессы и те, где это возможно, с помощью аналитических моделей, а также для других суб-построенных имитационных моделей. Этот комбинированный подход позволяет качественно новые классы систем покрытия, которые не могут быть исследованы с использованием только аналитическая и моделирование индивидуально.

Экспертные методы. Экспертные методы, используемые в теории безопасности конфиденциальной информации, могут быть разбиты на две части: первые методы направление стремимся создать базу данных экспертами анкеты защиты данных и информационной безопасности. В этом случае следующие допущения:

Стоимость затрат на защиту конкретных сведений не учитывается. Правомочность такого допущения оправдывается тем, что экономический ущерб от утечки конфиденциальной информации, как правило, многократно превышает стоимость мероприятий по ее защите, так как эти мероприятия применяются к ряду или всем сведениям и имеют постоянный характер.

- Оценка ущерба быть числовое значение в случае, когда вероятность утечки информации должна быть равна единице. Законность таких предположений оправдано тем, что важность информации определяется максимальным (потенциального) ущерба компании в результате утечки этой информации.

Оценка возможного ущерба от утечек конфиденциальной информации в следующей последовательности (общий подход):

- применяется к области бизнеса, информация о котором подлежат рассмотрению, соответствующий руководитель (лицо, ответственное за эту деятельность) разработаны предложения по формированию экспертной комиссии. В нее вошли эксперты, компетентные в отрасли. Если сфера охватывает сотрудничество предприятий, экспертная комиссия может быть включена в консультации с соответствующими менеджерами, представителями этих компаний. Количество экспертной комиссии зависит от сложности вопросов, но практика показывает, что команда должна состоять не менее чем из 5-7 экспертов. Формирование экспертной комиссии, утвержденной соответствующим приказом руководителя предприятия. Комитет назначается ее председателем и секретарем, который наделен подготовки справочной документации, анкет для членов комиссии, заседания протокол регистрации комитета.

- На заседании экспертов экспертной комиссии выдается анкеты. Эксперты по предложениям совместное решение о перечне информации об этой области деятельности, подлежащей экспертизе. Чтобы ускорить решение этого вопроса председатель комиссии может назначить отдельные эксперты выдержано список можно больше информации об этой сфере деятельности и сообщить об этом в заседании комиссии. Перечень сведений, чтобы быть опыт, принятой на заседании комитета вносятся в экспертов анкет. Экспертные оценки проводятся отдельно для каждого из информации. Эксперты совместно принять решение о возможных действиях конкурентов в случае их

осведомленности о рассматриваемой доказательств.

- Комиссия представила свои базовые данные о хозяйственной деятельности предприятий, а также одного из экономических индикаторов сферу (область) компании (например, договора или договоров), которые связаны с просматриваемой информации. Индикаторы могут быть доведены до относительных значений:

- Каждый эксперт в анкете прикреплена свое мнение об относительной снижением экономической эффективности работы предприятия в отношении каждого действий конкурентов, определяется общее относительное снижение экономической эффективности работы предприятия в результате всех возможных действий со стороны конкурентов.

- Окончательное значение ущерба, причиненного утечкой информации о результатах оценки Экспертного совета определяется путем усреднения все решения, связанные с оценкой экспертов. Критерием для классификации информации как конфиденциальной информации компании является состояние, при котором значение повреждений больше нуля. Уровни возможного ущерба от утечек конкретной информации характеризуют относительную важность этих данных.

- Экспертная комиссия формализованы протокол. Используя метод экспертных оценок включает в себя назначение конкретных экспертов "весовые коэффициенты" на основе их компетенции, провести повторные туры опросов, если есть много рейтинги удаления отдельных экспертов из оценках среднего значения группы.

Методы второго направления, связанного с использованием данных материалов для генерации баз знаний экспертных систем. Как правило, экспертные методы используются в качестве основы для методов математического моделирования, в результате большей точности в описании системы.

Анализ проблемы оценки ущерба предполагает, что:

- источники конфиденциальной информации являются люди, документы, публикации, технические носители, технические средства производства и занятости, продуктов и отходов;

- Каждый угроза влечет за собой некоторый ущерб - моральный или материальный, а также защиту и противодействие угрозе предназначен для уменьшения его стоимости;

- Математическое моделирование для изучения свойств систем функционирования можно разделить на аналитической, моделирования и комбинированные. Среди этих видов математического моделирования выбранной аналитического моделирования;

- При составлении математической модели необходимо учитывать большое количество внешних и внутренних факторов, которые в конечном итоге затрудняет модели;

- Для того чтобы определить заранее возможный ущерб, используют различные методы анализа. Среди них можно выделить следующие:

естественный эксперимент, ЛИХ, методы математического моделирования и экспертных методов.

2 Построение математической модели оценки ущерба от воздействия на конфиденциальную информацию внешних угроз

2.1 Концепция математической модели оценки ущерба конфиденциальной информации от внешних угроз

Информация, жертвенный без ресурса вычетов не могут быть непосредственно отнесены (этот вывод подтверждается тем, что в информационных процессах не закон сохранения). Поэтому невозможно определить ценность информации при рассмотрении ее модели используют только информацию (внутренний) уровень. Для информации о ценах вы хотите перейти по ссылке его содержание с ресурсом, который потребляется без остатка. Чтобы сделать это, необходимо связать содержание со значениями выше (внешний) уровень, для которого законы или есть сохранения более простые баланса отношений.

Таким образом величина целесообразно принять потенциальную ценность информации является обобщенным количественная характеристика мощности информационных достигается средств, потраченных без следа. Поскольку содержание комплекса мощи и многомерной, скалярного потенциала является простой подход, точность достаточна для сравнительной оценки эффективности (важность, значение) обеспечение "вещи", которые включают информацию.

Так, полученный таким образом информация цена не абсолютным, а относительным (субъективная, условный), т.е. действует только при определенных условиях, свойства, кроме частичной достаточности важно видимости свойство оценки. В связи с этим, совершенно ясно оценить ценность информации можно получить с помощью простой модели здание - раскрытая потенциал, который зависит от эффективности информационной безопасности. Она равна произведению величины общего потенциала информации, взятой до начала моделирования - U_obsch на вероятность несанкционированного доступа к конфиденциальной информации, как это определено математической модели работы системы – $P_{нсд}$

$$U_p = U_{общ} P_{нсд}, \tag{2.1}$$

Под общим потенциалом информации $U_{общ}$ будем понимать тот положительный эффект (материальный или моральный), который может быть получен при использовании её на указанном интервале времени. В этом случае формальная основа соперника как формальной основе соперника к несанкционированного доступа к информации и ее защиты является проблема максимин.

$$max_r min_z U_p(r, z, |S|), \quad (2.2)$$

где U_p – значение раскрытого потенциала;

r, z – стратегии по несанкционированному доступу к конфиденциальной информации и защиты информации, соответственно, реализуемые в условиях системы S [12].

2.2 Анализ внешних параметров модели оценки ущерба конфиденциальной информации от внешних угроз

Модель оценки Нанесенный не закрыт. Как вы знаете, в полной мере отражает реальность модель должна учитывать множество внешних параметров, то есть данные из модели оперативной обстановки. Но на практике, рассмотреть все возможные варианты, в той или иной степени повлиять на исход моделирования, это не представляется возможным или является настолько сложным и трудоемкой задачей, что моделирование себя становится нерентабельным задачей. Рассмотрим наиболее важные параметры, в значительной степени влияющие на исход моделирования, а также попытаться определить численные значения, которые будут оцениваться по этим параметрам.

Одним из основных внешних факторов можно выделить квалификации нападавшего: чем она выше, тем больше вероятность несанкционированного доступа. При одинаковых условиях, вероятность другого несанкционированного доступа будет больше атакующего с более высокой квалификации. Поскольку это значение не ясно регулируемых единиц и, более того, является абстрактным характеристика, то применяются к настоящему делу ограничить количество квалифицированного нападающего заключен в диапазоне от 0 до 1, где 0 указывает профессиональной неграмотности нападающего и одного из его полного профессионализма .

Другим важным параметром является время, затраченное на реализацию атакующий несанкционированного доступа. Чем больше время, тем больше шансов, что попытка увенчалась успехом, но тем больше вероятность, что злоумышленник пойман с поличным.

На практике для этой величины в нашей модели будем использовать Марковские процессы с дискретными состояниями и непрерывным временем, которые, как известно, в большинстве случаев характеризуются двумя параметрами интенсивности λ_i и μ_i, где параметр λ_i характеризует интенсивность прямых переходов между составляющими S_i системы S, а параметр μ_i, – обратных переходов между составляющими S_i (рисунок 2.1).

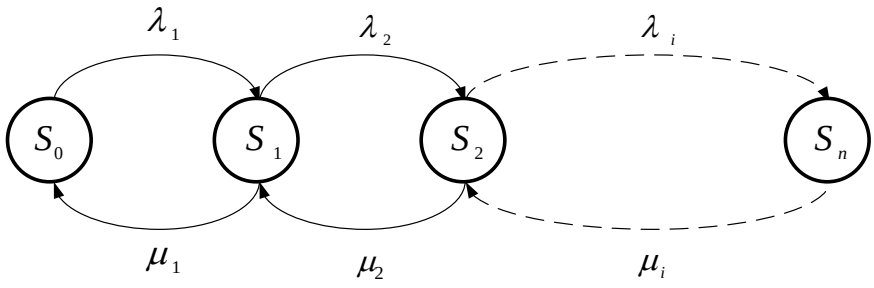


Рисунок 2.1 – Пример графа Марковского процесса

Кроме того, необходимо также учитывать количество нападавших. Чем больше число, тем больше вероятность случай несанкционированного доступа к объекту охраны. Когда оценка ущерба, в то время как несколько нападавших несанкционированного доступа. В нашем случае, этот факт будет учитываться при использовании проблемой, когда некоторые из потенциального ущерба, причиненного максимальная будут выбраны по наиболее квалифицированных.

Также следует отметить, что любая конфиденциальная информация имеет также физический компонент. Какие характеризует защиту конфиденциальной информации от физической стороны. Например, если информация в Интернете, это важная роль в несанкционированном доступе к конфиденциальной информации играет техническое оборудование нападавшего. Чем она выше, тем меньше заметны, легче и лучше она сможет реализовать угрозу. В математической модели для каждого из его компонентов должны быть определены так называемый энергетический вероятность обнаружения конфиденциальной информации, в зависимости от технического оснащения злоумышленника.

Помимо параметров, связанных с действиями злоумышленников, также используется в модельных параметров, связанных с различными законами распределения вероятностей. Значения этих параметров определяются с помощью статистических методов. Ограничения на этих параметров, связанных с распределением самих законов.

2.3 Разработка процедуры определения размеров ущерба вследствие утечки конфиденциальной информации

Определение размера ущерба в связи с распространением сведений, составляющих тайну, используя различные образцы является основой для принятия решения о необходимости ограничить доступ к данным и информации, оценки эффективности информационной безопасности.

Наиболее общей характеристикой в этом случае размер экономический ущерб. Методы определения масштабов ущерба, который может быть причинен безопасности или состояние в связи с распространением сведений,

составляющих тайну, зависит от следующих факторов:
- Направления деятельности, которая включает в себя информацию считается (экономического, научно-технического и т.д.);
- Степень неопределенности информации, используемой в оценке ущерба;
- Сфера проявлений повреждения (в конкретных областях, или комплекс в некоторых областях).

Рассмотрим модель для определения степени ущерба, применяемыми в ситуациях, когда информация относится к довольно узкой областью эта область ограничена проявления предрассудков и исходящих данных для оценки вполне определенное. В этом случае целесообразно применять метод, основанный на модели «знания-эффективности», что позволяет получить количественные оценки ущерба. В качестве методологической основы для определения масштабов ущерба в неопределенности исходной информации и районах ущерба целесообразно выбрать метод, разработанный TL Саати.

Представлено метод оценки размера ущерба, понесенного им в результате распространения сведений, составляющих тайну, на основе анализа влияния изменений в осведомленности противника (конкурента) этих результатов с выполнением объектов, подлежащих охраняемых - носители информации. Когда объекты анализируются защиты находятся в остром конфликте с самых важных объектов противника, результаты которого определяют эффективность защиты объектов, их живучесть, а также жизненно важные интересы заинтересованных сторон.

Для определения возможного ущерба в связи с распространением информации о защищаемом объекте выполняет определенные процедуры

Концепция процедур оценки ущерба конфиденциальной информации

Оценка априорного знания о противнике является задачей прогнозирования для «противника» характеристик объекта, а также оценку точности и достоверности прогноза. Источники информации для программирования являются: характеристики аналогичных объектов, опубликованные в открытой печати, передаваемые другим сторонам при проведении переговоров;

– характеристика аналогичных объектов соперника;

– технические, физические, экономические и другие ограничения на достижимые значения других характеристик защищаемых объектов;

– материалы, поступающие от служб безопасности организации, владеющим защищаемым объектом.

В качестве показателей оценки осведомленности соперника о защищаемых объектах могут использоваться:

– для сведений количественного характера – среднеквадратическая ошибка определения значения сведения (характеристики); отключение (смещение) математического ожидания значения; вероятность определения (измерения) значения с заданной точностью;

– для сведений качественного характера (например, наличие объекта или определенного свойства объекта) – вероятность правильного распознавания объекта; вероятность вскрытия данного сведения.

Оценка влияния распространения влияния сведений об объектах на осведомленность соперника. Такая оценка осуществляется путем сравнения истинных значений сведений, которые могут быть известны сопернику. Если ошибки определения сведений по результатам прогнозирования несущественны, то распространение сведений об объекте практически не повлияет на осведомленность соперника на них.

Оценка влияния распространения влияния информации об объектах на осведомленности противника. Такая оценка осуществляется путем сравнения истинные ценности информации, которая может быть известна противнику. Если ошибка в определении информации о результатах прогноза являются незначительными, распространение информации о практически без воздействия на сознания соперника к ним.

Предвидя возможные контрмеры против объекта защиты злоумышленник. Это осуществляется с помощью информации, доступной соперника путей и средств функций объекта и их возможного развития. Необходимо определить, какие контрмеры могут быть быстро реализованы в короткий период времени. Следует отметить, что соперник делает дополнительные контрмеры, если объект считается реальной угрозой для него (например, эффективность новых технологий конкурента значительно превышает эффективность существующих).

В жизненном цикле объектов должны быть защищены, как правило, происходит постепенное изменение сознания соперника невежества их характеристик до их полного и достоверного знания. Защищаемые обычно сложные по составу, можно охарактеризовать значительным количеством информации, таким образом, количество возможных вариантов (информационно государства) может быть большим противником.

В то же время, некоторые состояние сознания может незначительно отличаться от точки зрения, реализованной на основе их контрмер и прикладных с предубеждением. Таким образом, для того, чтобы уменьшить количество исследованных контрмер противника выбран ограниченное количество принципиально разной состояний сознания охраняемых объектов. Мы называем эти критическое состояние. Каждое критическое состояние сознания характеризуется набором (комбинированной) информации, необходимых для реализации по крайней мере один из контрмер.

Между различными состояниями информационно критических отношений набор приоритета и последовательности во времени в соответствии с расширением множества данных, характеризующих эти параметры. В результате представляет собой график изменений в осознании объекта (рис. 2.2).

Вершины графа соответствуют различным состояниям сознания, дуги - переходы из одного состояния в другое.

Начальное состояние графа соответствует отсутствию достоверной информации от соперника; Конечное состояние - его полное осознание защищаемого объекта. Контрмеры конкурентом для возможности их

одновременной реализации подразделяют на следующие классы:

– простые (для данного состояния осведомленности существует только одна контрмера);

– альтернативные (из нескольких вариантов контрмер одновременно может реализоваться только одна);

– обобщенные, реализуемые путем наращивания контрмер, принятых для более ранних состояний осведомленности (при реализации всех мер формируется обобщенная мера).

Отношения между различными контрмер отображаются в виде графика обобщенных контрмер путем строительства. Вершины графа соответствуют простой и обобщенной контрмер и дуг - включение обобщенных контрмер контрмер. Отношения между информационно и контрмер вариантов выглядят как дуг, соединяющих эти графы. Каждый из дуг, соединяющих различные состояния графа могут быть связаны с оценкой вероятности и момент перехода из одного состояния в другое.

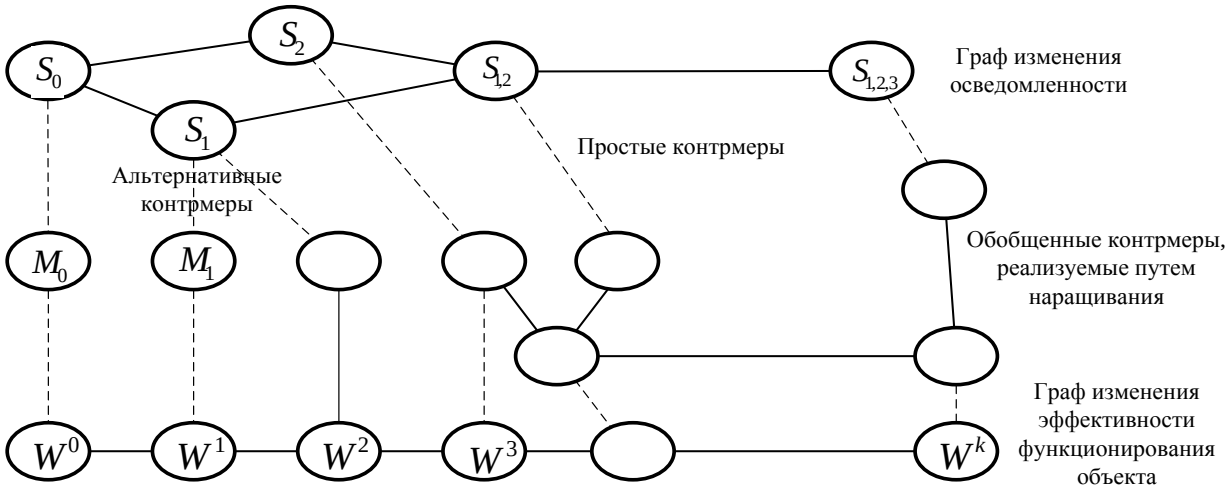


Рисунок 2.2 – Обобщенная графическая модель взаимосвязи состояния осведомленности соперника об объекте, соответствующих им контрмер и эффективность функционирования объекта

Моделирование влияния контрмер противника на производительность защищаемого объекта осуществляется с помощью следующих мер.

Оценка возможного снижения эффективности в зависимости от объекта контрмер противника при условии применения моделей функционирования охраняемых объектов путем изменения входных данных и параметров этих моделей. Для этого модель была чувствительна к изменениям в действиях противника, в зависимости от его знаний об объекте.

Для получения оценки воздействия осведомленности об эффективности своих операций и суммы убытков, возникающих моделировать процессы, отображаемые трех взаимосвязанных графов: информационно изменения,

реализации контрмер и изменений эффективного функционирования объекта. Содержание этих процессов заключается в следующем.

Последовательно к определенной дате достигается одно из состояний графа осведомленности в которых начинается процесс реализации соответствующих контрмер. При реализации этого противодействия достигнуто одно из состояний в графе изменяет функционирование объекта. Время достижения заданного состояния в графе изменяет эффективность объекта определяется как количество времени, необходимое для достижения состояния соответствующей противника осведомленности, и время, необходимое для осуществления соответствующих государственных контрмер.

Результаты расчетов эффективности функционирования объекта при различных информационно противника упорядоченной по значению и эффективности отображается в виде графика изменения в функционировании объекта.

Таким образом, Рисунок 2.2 иллюстрирует процесс изменения эффективности объекта, который будет защищен от изменений в осведомленности соперника его.

Оценка ущерба в связи с низкой эффективностью защищаемого объекта могут быть основаны на двух методов.

Первый метод полезен, когда объекты, которые будут защищены может быть несколько. Она состоит в выявлении дополнительных материальных затрат, необходимых для восстановления потерянного эффективность объекта, применяя дополнительное количество объектов, которые будут защищены. Нанесенный значение при восстановлении эффективности за счет использования дополнительных средств рассчитывается по формуле

$$U = NN_{add}(C + C_{ancxp}T_{cxp}), \qquad (2.3)$$

где N – объем производства рассматриваемых объектов защиты;

N_{add} – необходимое увеличение числа объектов защиты для восстановления утраченной эффективности, рассчитывается с использованием моделей оценки эффективности объектов;

C – стоимость создания объекта защиты;

C_{ancxp} – стоимость готовой эксплуатации объекта защиты;

T_{cxp} – продолжительность эксплуатации объекта защиты.

Второй метод применим для оценки защиты от вандализма отдельных объектов, и на основе оценки денежных затрат на создание защиты необходимую эффективность проектирования. При снижении этой эффективности за счет увеличения информированности и принятия противника и контрмер считается, что часть затрат на создание объекта пропорционально снижению эффективности объекта, и отражает стоимость потерянного повреждения.

В этом случае величина ущерба ориентировочно рассчитывается по

формуле

$$U = NC\delta W \ , \qquad (2.4)$$

где $\delta W = \frac{\Delta W}{W}$ – относительное снижение эффективности объекта вследствие возрастания осведомленности соперника о его характеристиках;

W – проектная эффективность объекта;

ΔW – ожидаемое снижение эффективности объекта вследствие возрастания осведомленности соперника и принятия им контрмер.

Материал в вопросе основные элементы дизайна для изготовления продуктов, используемых в ситуациях противостояния и конкуренции.

Прогнозируемое изменение в априорного знания о материальном конкурента во время его жизненного цикла. Результаты представлены в виде матрицы

$$P_n = |P_{ki}^n|, k = 1, 2, \dots, K, i = 1,2, \dots, I \qquad (2.5)$$

где P_{ki}^n – оценки в виде вероятностей определения сведений;

k – количество сведений о материале;

i – число этапов жизненного цикла материала.

Пример представления оценок приведен в таблице 2.1

Т а б л и ц а 2.1 – Представление оценок в виде вероятностей определения сведений

Сведения о материале	Значения показателя априорной осведомленности на тапах жизненного цикла				
	Исследования	Разработка	Испытания	Производство	Примечание
Назначение	0	0,3	0,6	0,65	0,8
Рецептура	0,2	0,2	0,5	0,5	0,6
Технология создания	0	0	0,7	0,8	0,9

– Определяются возможные состояния осведомленности злоумышленника о материале. Результаты представляются в виде матрицы

$$S = |\Delta mk|, m = 1,2,\dots,M \ , \qquad (2.6)$$

Прогноз возможных путей и средств поражения (уничтожения) элементов дизайна продукта в получении информации о материале, из которого продукт изготовлен. Ущерб от снижения эффективности (живучести) продукции в их применении оценивается в денежном выражении, как нерационально используется стоимость создания продукта, который потерял часть своей доли эффективности проекта, включая затраты на создание материально.

Информация о характеристиках материалов и технологиях их создания может быть использована для воссоздания и применения подобного материала в изделиях конкурента соответствующего ущерба.

Результаты прогнозирования состояния осведомленности о материале и возможные последствия представлены в таблице 2.2.

– Прогнозируется время реализации контрмер. Результаты прогнозирования представляются в виде оценок среднего времени и среднеквадратического отклонения времени реализации контрмер.

Т а б л и ц а 2.2 – Результаты прогнозирования состояния осведомленности о материале и возможные последствия

№ состояния	Известные сведения (нумерация в соответствии с таблицей 1)			Возможные последствия
1	2	3	4	5
1.	1	0	0	-
2.	1	1	0	Снижение живучести изделий
3.	1	1	1	Снижение конкурентоспособности

– Расчетное максимальное (без защитных мер) и минимальная (с защитой) значения вероятности определить информацию о материале на разных стадиях жизненного цикла материала (с мерами / без защитных мер) представлены в таблице 2.3.

Т а б л и ц а 2.3. – Максимальные и минимальные значения вероятностей определения сведений о материале на различных стадиях жизненного цикла

Сведения о материале	Вероятности определения сведений				
	Исследования	Разработка	Испытания	Производство	Примечание
1	2	3	4	5	6
Назначение	0/0	0/0	0/0,3	0,1/0,5	1/1
Рецептура	0/0	0/0,2	0,1/0,5	0,1/0,7	0,1/0,9
Технология	0/0	0/0,1	0/0,3	0,1/0,7	0,5/1

– Вычисляются вероятности определения конкурентом k-го сведения к i-му этапу жизненного цикла материала (с мерами и без мер защиты)

$$P_{ki} = 1 - (1 - P_{ki}^{I})(1 - P_{ki}^{N}) \qquad (2.7)$$

где P_{ki} – вероятность определения сведений к i-му этапу жизненного цикла материала в результате утечки информации по техническим каналам;

P_{ki}^{N} – прогноз априорной осведомленности.

$$P_{ki}^{I} = 1 - \prod_{\xi-1}^{\xi+1} 1 - P_{K\xi}\ , \qquad (2.8)$$

здесь $P_{k\xi}$ – вероятность определения k-го сведения на ξ-м тапе жизненного цикла (см. таблицу 2.1).

Результаты приводятся в виде матрицы

$$P_{\Sigma} = P_{ki}\ , \tag{2.9}$$

и в виде таблицы, аналогичной таблицы 2.1.

– Вычисляются вероятности достижения конкурентом m-го варианта осведомленности о материале к *i*-му этапу его жизненного цикла

$$P_{mi}^{S} = 1 - \prod_{k-1}^{k} (P_{ki}^{N})^{\Delta mk}\ , \tag{2.10}$$

где Δmk – значения элементов таблицы 2.2.

Результаты вычислений представляются в виде матрицы

$$P_{S} = P_{mi}^{S}\ , \tag{2.11}$$

Вероятность достижения состояния сознания к различным стадиям жизненного цикла материала (с мерами / без защитных мер) представлены в таблице 2.4.

Т а б л и ц а 2.4 - Вероятности достижения состояния осведомленности к различным этапам жизненного цикла материала (с мерами/без мер защиты)

№ состояния	Вероятности определения сведений				
	Исследования	Разработка	Испытания	Производство	Примечание
1	2	3	4	5	6
1	0,1/0,2	0,2/0,5	0,4/0,6	0,8/0,9	1,0/1,0
2	0,05/0,1	0,1/0,3	0,3/0,4	0,6/0,9	0,9/1,0
3	0,03/0,05	0,05/0,07	0,2/0,3	0,5/0,8	0,8/1,0

2.4 Разработка математической модели оценки ущерба конфиденциальной информации от внешних угроз

При определении ущерба от утечки информации необходимо определить понятие общей мощностью и создать модель для ее определения. С концепция общей мощностью неразрывно связано понятие ценности информации.

Под ценности информации, что мы понимаем позитивный эффект (моральный или материальный), который может быть получен при использовании его в указанное время. Как видно из определения значения, это

значение не является постоянной и в различные периоды времени может варьироваться в разных диапазонах. Например, при создании стоимости чипа информацию нового поколения о своей архитектурой очень высока, но со временем появление аналогов или рассекречивания своей архитектурой и ее значение уменьшается до определенного уровня. Потенциал является характерной интервал и точкой.

Большинство реальных объектов, как правило, распределены по времени. Не является исключением и потенциал. Как вы знаете, нормальное распределение вероятностей называется непрерывная случайная величина, которая описывается плотности

$$f(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(t-\alpha)^2}{2\sigma^2}} \tag{2.12}$$

Графиком плотности нормального распределения является следующая нормальная кривая (рисунок 2.5):

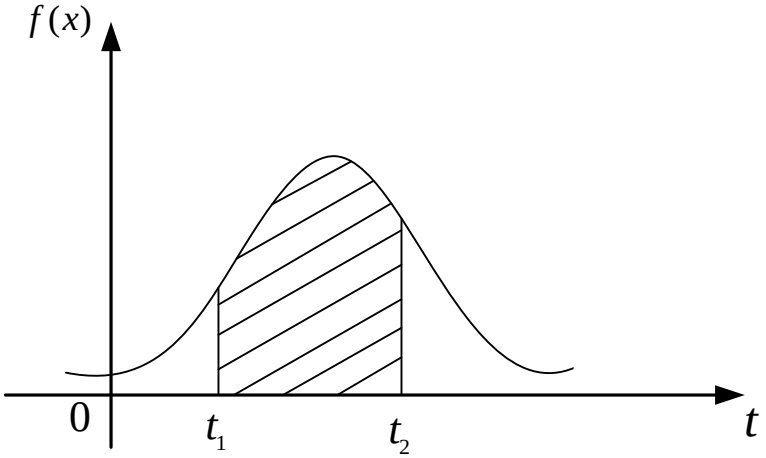


Рисунок 2.5 – График нормальной кривой

Определить потенциал, что для ее расчета на интервале [t1, t2] должны принять определенный интеграл в том же диапазоне функции плотности нормального распределения, умноженной на начальной информации о стоимости. Кроме того, необходимо учитывать тот факт, что функция плотности нормального распределения сдвига вправо вдоль оси x берет свое начало точку (0,0), а также исходный потенциал равен исходному значению информации вам нужно поднять начало кривой в точке (0, 1), что соответствует функции F (X) 1 Таким образом, подводя итог всему вышесказанному, для расчета общий потенциал Uobsch использовать следующую формулу

$$U_{\text{общ}} = \text{C} \int_{t_1}^{t_2} [f(t+1)]dt, \tag{2.13}$$

где C – начальная стоимость информации;

t_1, t_2 – границы временного интервала моделирования;

f(x) – функция плотности вероятности.

При определении потенциал информации, которую вы должны знать 4 параметра: α и σ, определяющие форму кривой и T1, T2 - определение интервала расчет. Если параметры T1, T2 будут различными для различных расчетов, α и σ прикреплены к этой информации и, следовательно, правильной идентификации в значительной степени определяет правильность полученных данных. Среди параметров α и σ наибольшее значение является параметром σ. Его изменение влияет на ординат максимум потенциала: с увеличением σ максимума уменьшается ординат потенциала и кривой сам становится более плоским, т.е. сокращается до оси x; с уменьшением потенциальная кривая становится более остроконечная и растягивается в положительном направлении оси y.

Физический смысл параметра σ - это максимальная сумма прибыли, которую можно получить, используя информацию. Таким образом, для определения параметра σ на практике различные статистические методы определения максимальной прибыли от использования конфиденциальной информации, а затем подобрать параметр σ таким образом, что она встречается с результирующее значение. В свою очередь также являются важными α параметров: при увеличении параметра α график сдвигается вправо по горизонтальной оси, с уменьшением - влево по горизонтальной оси.

Таким образом, перед выбором параметр моделирования α так, чтобы кривая e (т +1), где F (T) - функция плотности нормального распределения, был свой начальную точку (0,1).

Для формального решения задачи необходимо определить: потенциал и его зависимость от содержания конфиденциальной информации; Содержание стратегии несанкционированного доступа к конфиденциальной информации и ее защиты. Когда общая емкость информации Uobsch его тотальность типичные объекты, потенциалы определяются математических моделей их функционирования на основной цели. Потенциал для стоимости является эффективность объектов, определенных для фиксированных условий S.

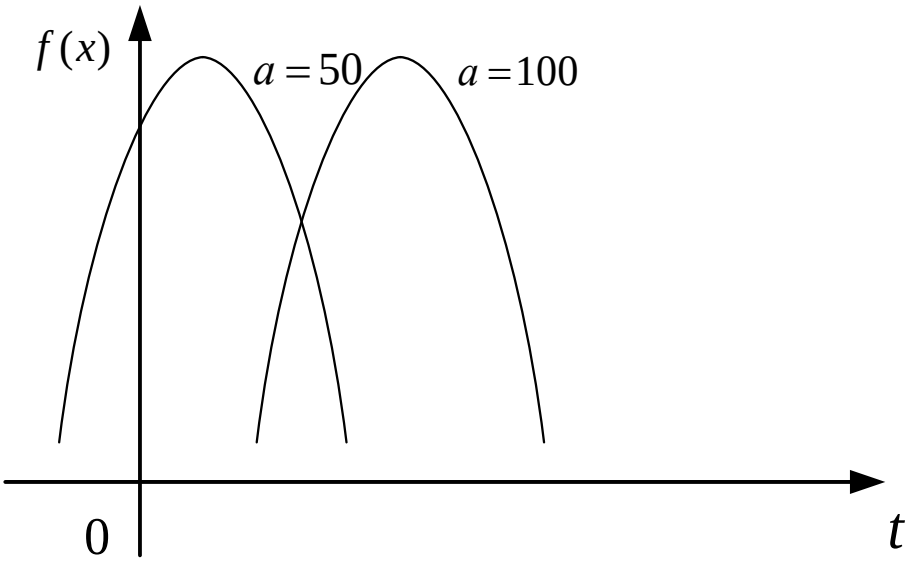


Рисунок 2.6 – Графики нормальной кривой при различных значениях α

Математические модели требуются не функционирует для всех типов объектов, и лишь немногие - опорные потенциалы принимаются за единицу. Для всех остальных типов объектов соизмеримы коэффициенты относительно опорной путем сравнения сходства функционирующих. Потенциал информация представлены с потенциалов составляющих его типов объектов.

Таким образом, содержание конфиденциальной информации определяется составом и характеристиками типичных объектов их функционирования. Вместе они могут считаться набор функций, описывающих состав и функционирование групп рассмотренных типичные объекты, что справедливо в соответствии с гипотезой. В нем говорится, что содержание любой информации, в том числе хранятся в виде записей, с любой точностью можно представить набор характеристик - "сгустки" информации.

Скорость утечки определяется информационной индекс утечки конфиденциальной информации с помощью набора атрибутов, который может быть риск несанкционированного доступа к конфиденциальной информации. В этой математической модели необходимо несанкционированного доступа, в том числе модели обнаружения энергии, динамической модели несанкционированного доступа и последовательной интерпретации данных.

Построить математическую модель. Защита данных выполняется тремя способами: исключение означает получения от правильной работе; ограниченный доступ к источникам утечки информации; отвлечение средств для закупки ложные источники. Стратегия обороны целесообразно сочетание этих методов, оправдывая "эффект-затраты».

Рассмотрим оценку убытки, связанные с несанкционированным доступом к конфиденциальной информации в автоматизированной системе - Акустические системы. Пусть АС включает в себя уровни K, каждая из которых состоит из N подсистем (J = 1, N), где параметр A ^ характеризует интенсивность прямых переходов между компонентами Si системы S, а

параметр μi, - обратных переходов (рис. 2.7). Каждая из подсистем с требуемой детальностью описывается совокупностью признаков $\{\gamma_i\}$. Среди признаков существует подмножество $\{\gamma_j\}\epsilon\{\gamma_i\}$ признаков распознавания. Тогда механизм дифференцированной защиты информации формально задается выражением (2.14)

$$max_r min_a \sum_{i=1}^{n} U_i(\gamma_i) P_{\text{нсд}i}[r(\gamma_i) z(g_{il}) |S|], \qquad (2.14)$$

где $U_i(\gamma_i)$ – потенциал j–ой подсистемы АС;

$P_{\text{нсд}i}[r(\gamma_i) z(g_{il}) |S|]$ – вероятность благополучного исхода несанкционированного доступа к конфиденциальной информации, реализуемая в i-ой подсистеме АС злоумышленниками по совокупности признаков γ_i;

g_{il} – совокупность ресурсов l-го типа, используемых для защиты информации i-ой подсистеме АС .

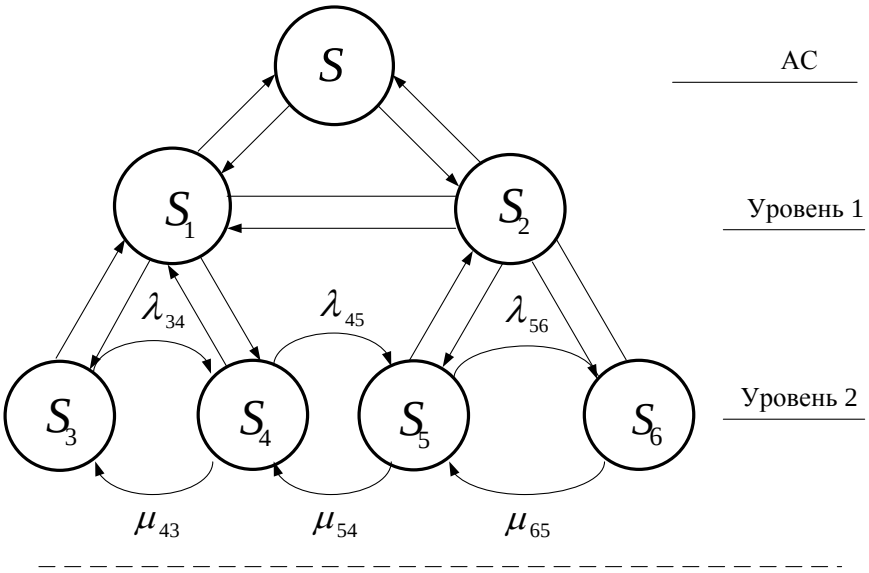


Рисунок 2.7 – Структурная схема автоматизированной системы

Вероятность несанкционированного доступа к конфиденциальной информации в i-ой подсистеме АС равна:

$$P_{\text{нед}}[\gamma] = P_{\text{нед}}\{\gamma'_j\} P_{\text{расп}}\{\gamma'_j\}, \qquad (2.15)$$

где $P_{\text{нед}}\{\gamma'_j\}$– вероятность несанкционированного доступа к конфиденциальной информации злоумышленниками при их действии в *j*–ой подсистеме АС;

$P_{\text{расп}}\{\gamma_i\}$ – вероятность распознавания информации по совокупности признаков распознавания $\{\gamma_i\}$.

Марковского процесса несанкционированного доступа и имеет вид

$$P_{нсд}\{\gamma_i\} = |P_k J_o J_o' \varpi(z)| dtdz P_{обн}(y_i) \qquad (2.16)$$

где P_k – финальная вероятность перехода из состояния в состояние Марковской_цепи;

$\varpi(z)$ – плотность вероятности времени нахождения в состоянии (на практике было установлено, что она описывается распределением Вейбулла со значениями показателя масштаба b = 0,02..0,5 и показателя формы c = 0,3..0,7);

$P_{обн}(y)$ – вероятность энергетического обнаружения признака (определяется физикой подсистемы АС).

Для определения Рк - ограничение вероятности перехода из одного состояния цепи Маркова из рисунке 2.7. Граф состояний показано на этом рисунке состоит из ряда взаимосвязанных состояний, когда состояние Si указывает, что имело несанкционированный доступ к подсистеме ввода-го. Выше, а также вид на графа состояний предполагает, что уровень каждого громкоговорителя не что иное, как процесс "смертном разведения" (рис. 2.8).

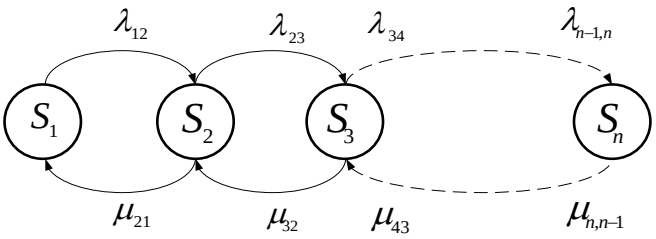


Рисунок 2.8 – Общий вид уровней автоматизированной системы

В зависимости от типа разметки государственной графика однородного марковского процесса, матрица λ переход плотность вероятности S система из одного состояния в другое является:

$$\lambda = \begin{pmatrix} -\lambda_{12} & \mu_{21} & 0 & \dots & 0 \\ 0 & -(\mu_{21}+\lambda_{23}) & \mu_{22} & \dots & 0 \\ 0 & \lambda_{23} & -(\mu_{32}+\lambda_{34}) & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \mu_{n,n-1} \\ 0 & 0 & 0 & 0 & -\mu_{n,n-1} \end{pmatrix}$$

Эта матрица соответствует однородной системы линейных алгебраических уравнений для вектора вероятностей состояний предельных:

Первый уровень системы мы записали:

$$\lambda_{12} p_1 = \mu_{21} p_2, \qquad (2.26)$$

значит, второе уравнение может быть представлено в виде:

$$\lambda_{23}p_2 = \mu_{32}p_3. \tag{2.27}$$

Продолжив аналогичные выкладки, приходим к следующим соотношениям:

$$\lambda_{k,k+1}p_k = \mu_{k+1,k}p_{k+1},\ k = \overline{1,n-1}, \tag{2.28}$$

или, что то же самое,

$$p_{k+1} = \frac{\lambda_{k,k+1}}{\mu_{k+1,k}}p_k.\ \ k = \overline{1,n-1}. \tag{2.29}$$

Таким образом,

$$\begin{cases} p_2 = \dfrac{\lambda_{12}}{\mu_{21}}p_1, \\ p_3 = \dfrac{\lambda_{23}}{\mu_{32}}p_2 = \dfrac{\lambda_{12}\lambda_{23}}{\mu_{21}\mu_{32}}p_1, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ p_n = \dfrac{\lambda_{n-1,n}}{\mu_{n,n-1}}p_{n-1} = \dfrac{\lambda_{12}\lambda_{23}\lambda_{34}\dots\lambda_{n-1,n}}{\mu_{21}\mu_{32}\mu_{43}\dots\mu_{n,n-1}}p_1 \end{cases} \tag{2.30}$$

Для окончательного нахождения вероятности состояний предельные, мы используем тот факт, что граф состояний является полная группа и, соответственно, на основе имущества:

$$\sum_{k=1}^{n} p_k = 1, \tag{2.31}$$

$$p_1 = \left(1 + \sum_{k=1}^{n-1}\prod_{j=1}^{k}\frac{\lambda_{j,j+1}}{\mu_{j+1,j}}\right)^{-1}, \qquad k = \overline{1,n-1}. \tag{2.32}$$

Подставляя это значение p_1 в систему (2.30), получаем:

$$p_{k+1} = \prod_{j=1}^{k}\frac{\lambda_{j,j+1}}{\mu_{j+1,j}}\left(1 + \sum_{k=1}^{n-1}\prod_{j=1}^{k}\frac{\lambda_{j,j+1}}{\mu_{j+1,j}}\right)^{-1}, \qquad k = \overline{1,n-1}. \tag{2.33}$$

Переходный процесс марковского процесса для соответствующей

определенной на моделировании, соответствующих физическому содержанию задачи.

P_rasp вероятность (y) и {Y} алгоритмы P_rasp Байеса определяется структурное признание. Используется в качестве признаков {y ^ '} накопили статистику для формального представления объектов для признанных алфавиты используются кадры искусственного интеллекта.

2.5 Выводы

Построить математическую модель для оценки ущерба конфиденциальной информации от внешних угроз показал, что:

– Субъективная оценка определяется путем умножения значения потенциалов типичных объектов информации на вероятность их открытия.

– возможен вскрытие определяется сочетанием аналитических и имитационных моделей, разработанных на основе физических особенностей проблемы на основе теории марковских процессов, структурных рамок и признания искусственного интеллекта.

– На основе анализа внешних параметров модели следующие задачи: анализ потенциальных угроз и характера методов оценки, модель оценивает ущерб от внешних параметров, математическая модель оценки ущерба, анализ влияния входных параметров на ущерб.

– Для определения возможного ущерба в связи с распространением информации о защищаемом объекте выполняет определенные процедуры.

– Оценка ущерба основана на двух методах: защита на нескольких площадках и защиты отдельных объектов.

3. Реализация и исследование математической модели оценки ущерба конфиденциальной информации от внешних угроз

3.1 Алгоритм построения математической модели оценки ущерба конфиденциальной информации от внешних угроз

Исследует, как с математической модели для определения оценки ущерба от внешних угроз к конфиденциальной информации:

Выбрать количество экспериментов *N*.

- Выбрать параметры α, σ и *C* для расчета потенциала.
- Определить значение общего потенциала – $U_{общ}$:

$$U_{общ} = C\int_{t_1}^{t_2}\frac{1}{\sigma\sqrt{2\pi}}e^{-(t-\alpha)^2/2\sigma^2}dt, \quad (3.1)$$

- Для каждого из *N* экспериментов определить количество подсистем АС.
- Выбрать параметры прямых $\lambda_{i,j}$ и обратных $\mu_{i,j}$ переходов между подсистемами автоматизированных систем, а так же финальные вероятности перехода $P_{обн}$ и $P_{расп}$ между подсистемами автоматизированных систем.
- Рассчитать на основе введенных параметров вероятности НСД – $P_{нсдj}$:

$$P_{нсдj}\{y_t\} = [P_k\int_0^{\lambda}\int_0^{\mu}\varpi(t)\varpi(z)dtdzP_{обн}(y_i) \quad (3.2)$$

- Вычислить итоговую вероятность НСД – $P_{нсд}$:

$$P_{обн}\left\{\gamma'_j\right\} = \frac{\sum_{i=0}^{L_j}\{P_{нсдj}\{\gamma_i\}P_{расп}\{\gamma_i\}\delta(\gamma_i,m)\}}{L_j}P_{гр}\left\{\gamma'_j\right\} \quad (3.3)$$

- На основе найденных значений общего потенциала $U_{общ}$ и $P_{нсд}$ определить величину ущерба – U_p:

$$U_p = P_{общ}P_{нсд}, \quad (3.4)$$

- Среди найденных значений величин ущерба выбрать максимальное $\max(U_n)$.

3.2 Анализ влияния входных параметров модели на величину ущерба

Любая модель вычисляет значения выходных параметров, основанных на любой вход или начальных значений. В нашем случае, входной являются следующие параметры: P_obn, P_rasp, Аг, J ¬, μi, J, σ, а, с, б, выводится в качестве параметра, характеризующего величину ущерба - раскрытый потенциал.

Рисунок 3.1 – UML-диаграмма математической модели оценки ущерба

Рассмотрим зависимость выходных параметров модели по отношению к изменениям в исходных данных.

Чтобы это исправить, все значения входных параметров, за исключением теста, и оценить их влияние на конечный результат моделирования.

Параметры α, σ влияет на количество повреждений, и значения этих параметров выбираются для конкретного случая и один раз в течение периода моделирования не изменяются. Таким образом, на основе поведения

потенциальных объяснений, когда изменение этих параметров, сумма ущерба влияет только параметр σ: чем он меньше, тем больше значение от общей емкости и, следовательно, более величина ущерба.

Параметры, используемые в модели в качестве переменных, характеризующих техническое оборудование и опыт нападающего. Чем выше значение этих параметров, тем больше величина повреждений, о чем свидетельствует соответствующих расчетов, приведенных в таблице 3.1 и таблице 3.2.

Т а б л и ц а 3.1 – Зависимость величины раскрытого потенциала от изменения технического оснащения злоумышленника

Параметры	Значения								
$P_{обн}$	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
U_p	4737	9474	14211	18948	23685	28422	33159	37896	42633

Из рисунка 3.2 видно, что чем выше техническое оснащение злоумышленника ($P_{обн}$), тем выше вероятность несанкционированного доступа и, как следствие, и тем выше величина ущерба.

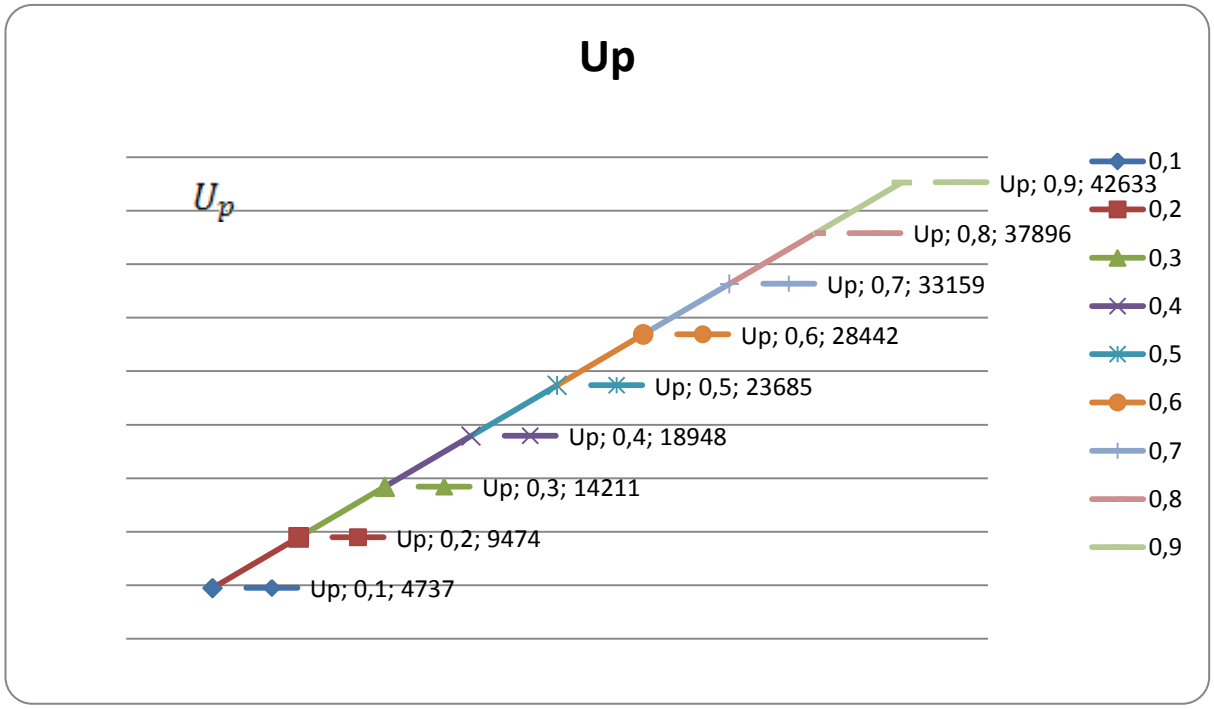


Рисунок 3.2 – Зависимость величины раскрытого потенциала от изменения технического оснащения злоумышленника

Из рисунка 3.3 видно, что чем выше квалификация злоумышленника ($P_{расп}$), тем выше вероятность несанкционированного доступа и, как следствие, тем выше величина ущерба.

Т а б л и ц а 3.2 – Зависимость величины раскрытого потенциала от изменения квалификации злоумышленника (λ=48, μ=30, c=0.5, b=0.2, $P_{расп}$=0.8)

Параметры	Значения								
$P_{расп}$	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
$U_р$	5329	10658	15987	21316	26646	31975	37304	42633	47962

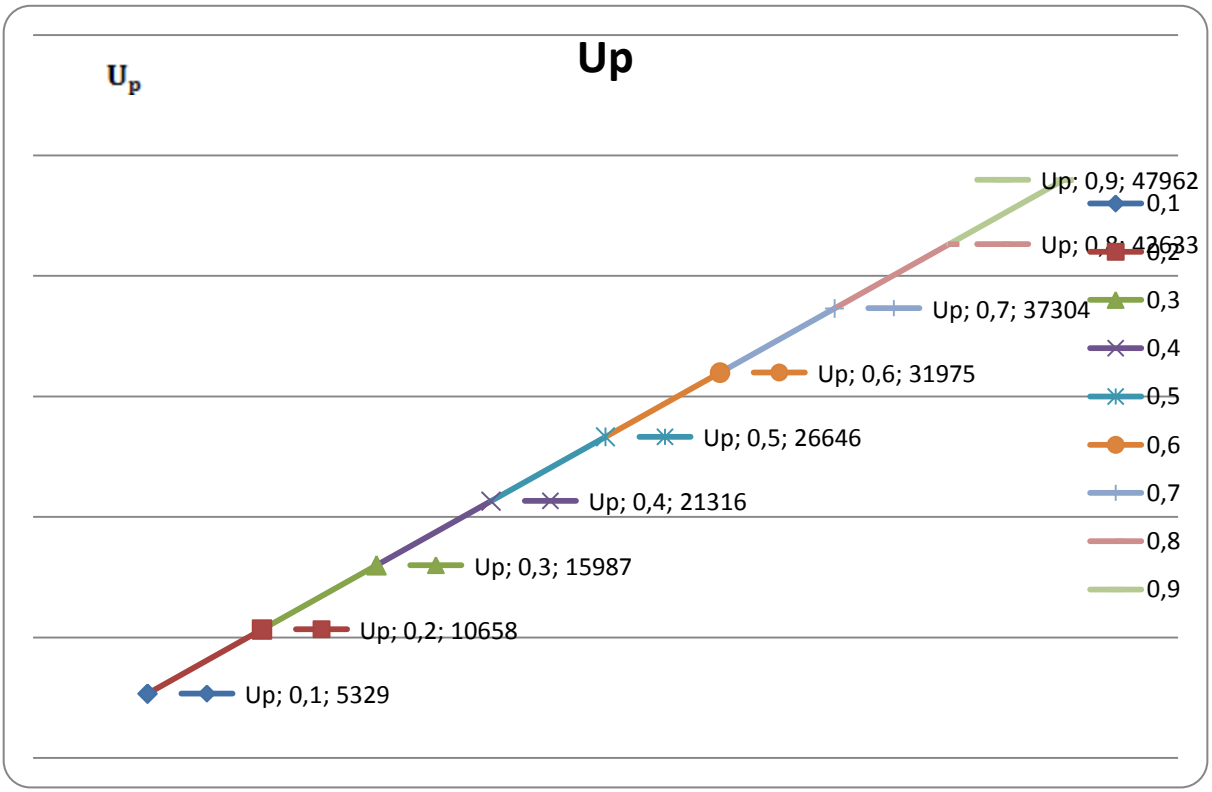


Рисунок 3.3 –Зависимость величины раскрытого потенциала от изменения квалификации злоумышленника

Параметры с, Ь. Оба параметра, б используется в модели для описания функции распределения Вейбулла, которые характеризуют плотность времени, находя нарушителя в подсистеме при осуществлении им угрозы несанкционированного доступа. Во-первых, рассмотрим поведение, когда параметр б. Fix оставшиеся варианты на следующих марок P_obn = 0,9, P_rasp = 0,9, λ = 15, μ = 5, c = 0,3, U_obsch = 500000, получим следующие результаты, показанные в таблице 3.3.

Из рис 3,4 показывает, что с ростом б значений наблюдается падение раскрыты потенциал, и для различных значений падения происходит по-разному: при c = 0,3 происходит быстрее, чем, например, если c = 0,5; c = 0,7 падение почти не происходит

Теперь рассмотрим поведение при изменении параметра с. Как и в предыдущем случае, зафиксируем параметры на следующих отметках:

Т а б л и ц а 3.3 – Зависимость величины раскрытого потенциала от изменения параметра *b* функции распределения Вейбулла

Параметры	Значения									
b	0,2	0,068	0,116	0,164	0,212	0,26	0,308	0,356	0,404	0,452
U_p	89830	87410	85100	83050	81220	79580	78090	76720	75470	74300

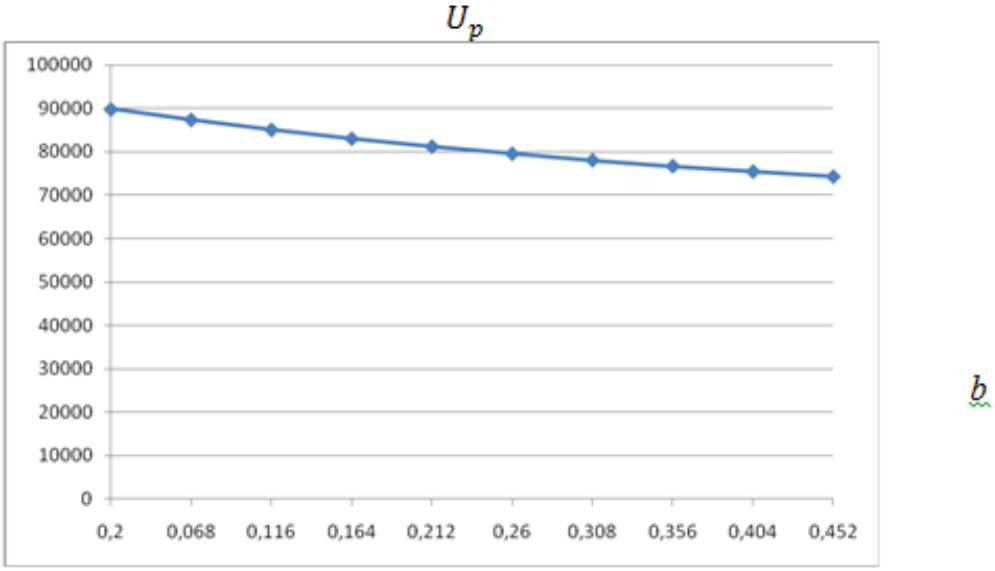


Рисунок 3.4 – График зависимости величины раскрытого потенциала от изменения параметра *b* функции распределения Вейбулла

Таким образом, как показано на рисунке 3,5, с увеличением параметра также увеличивает значение раскрытым потенциалом, таким образом, тем больше значение параметра B, тем острее увеличения стоимости раскрытым потенциалом. Теперь рассмотрим поведение суммы ущерба, когда параметры μ и λ. Для этого фиксируем другие параметры. Пусть Pobn = 0,9, Prasp = 0,9, c = 0,3, б = 0,04, U ¬ малыш = 500000, то изменения μ, получить повреждения приведены в таблице 3.5.

Таким образом, из расчетов показывает, что увеличение параметра λ, получаем первую иглу до определенного значения, после чего рост суммы ущерба прекращается; иначе в случае с параметром μ: увеличение этого параметра резкое снижение стоимости величины ущерба до определенного значения, после чего постепенное снижение суммы ущерба до 0%.. Таким образом, увеличивая вероятность несанкционированного доступа к параметрам λ увеличивается, что в свою очередь тесно приближается к 100%. Соответственно, увеличение параметра μ уменьшает вероятность несанкционированного доступа.

Т а б л и ц а 3.4 – Зависимость величины раскрытого потенциала от изменения параметра *c* функции распределения Вейбулла

Параметры	Значения									
C	0,3	0,34	0,38	0,42	0,46	0,5	0,54	0,58	0,62	0,66
U_p	31330	32710	33770	34560	35120	35510	35760	35930	36030	36090

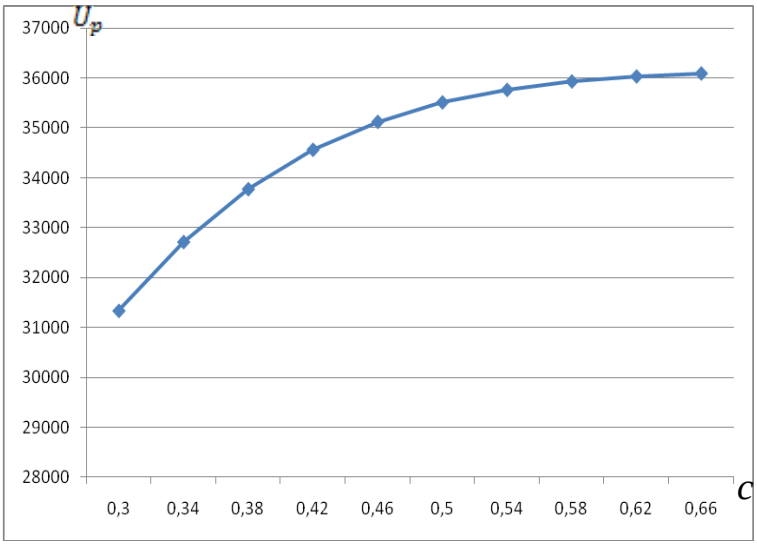


Рисунок 3.5 – График зависимости величины раскрытого потенциала от изменения параметра *c* функции распределения Вейбулла

Таким образом, из расчетов показывает, что увеличение параметра λ, получаем первую иглу до определенного значения, после чего рост суммы ущерба прекращается; иначе в случае с параметром μ: увеличение этого параметра резкое снижение стоимости величины ущерба до определенного значения, после чего постепенное снижение суммы ущерба до 0%.. Таким образом, увеличивая вероятность несанкционированного доступа к параметрам λ увеличивается, что в свою очередь тесно приближается к 100%. Соответственно, увеличение параметра μ уменьшает вероятность несанкционированного доступа.

Т а б л и ц а 3.5 – Зависимость величины раскрытого потенциала от изменения параметра интенсивности действий злоумышленника μ

Параметры	Значения									
μ	1	10	20	30	40	50	60	70	80	90
U_p	67815	72622	71855	68946	64173	58470	52726	47442	42797	38795
μ	100	110	120	130	140	200	300	500	700	
U_p	35371	32439	29916	27734	25833	18222	12176	7309	5221	

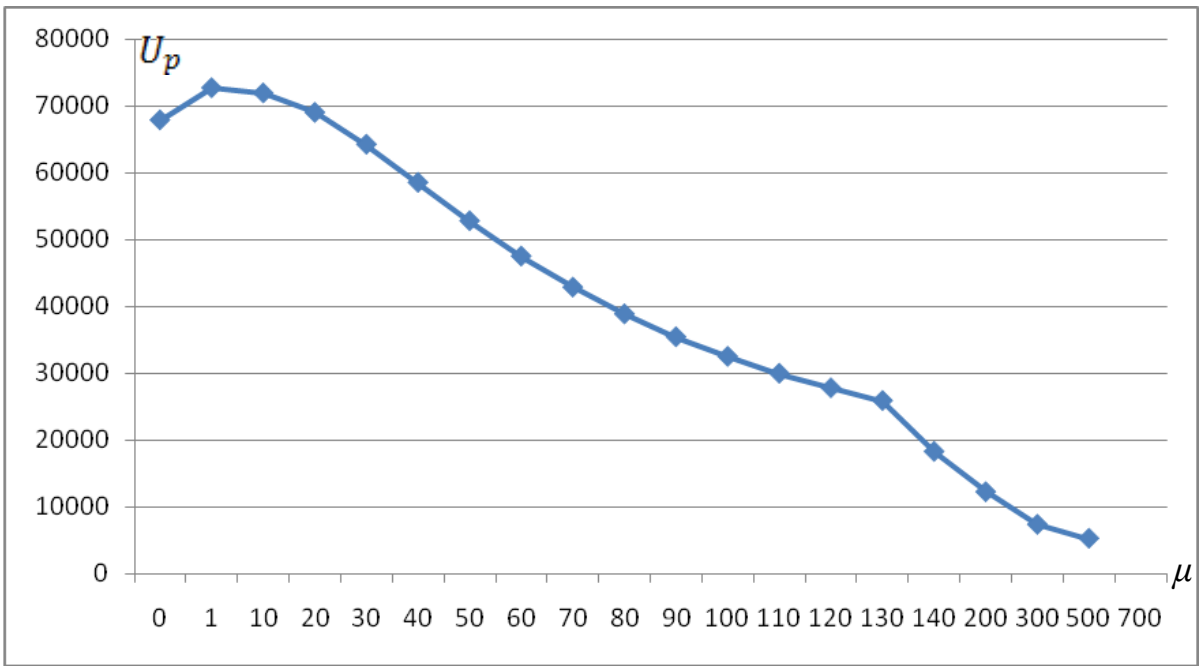


Рисунок 3.6 – График зависимости величины раскрытого потенциала от изменения параметра интенсивности действий злоумышленника μ

Теперь при тех же значениях $P_{\text{обн}} = 0.9$, $P_{\text{эн}} = 0.9$, $c = 0.3$, $b = 0.04$, $U_{\text{общ}} = 500000$ и при μ =50, изменяя λ получим результаты приведенные в таблице 3.6:

Таким образом, из расчетов показывает, что увеличение параметра λ, в стационарных условиях другие параметры, получаем первую иглу до определенного значения, после чего рост суммы ущерба прекращается; иначе в случае с параметром μ: увеличение этого параметра резкое снижение стоимости величины ущерба до определенного значения, после чего постепенное снижение суммы ущерба до 0%.. Таким образом, увеличивая вероятность несанкционированного доступа к параметрам λ увеличивается, что в свою очередь тесно приближается к 100%. Соответственно, увеличение параметра μ уменьшает вероятность несанкционированного доступа

Т а б л и ц а 3.6 – Зависимость величины раскрытого потенциала от изменения параметра интенсивности действий злоумышленника λ (λ = 48, μ=30, c = 0.5, b = 0.2, $P_{\text{обн}} = 0.9$)

Параметры	Значения									
λ	1	10	20	30	40	50	60	70	80	90
U_p	1461	14598	28781	41387	51346	58470	63266	66410	68465	69821
λ	100	110	120	130	140	200	300	500	700	
U_p	70730	71352	71786	72095	72319	72874	73041	73081	73086	

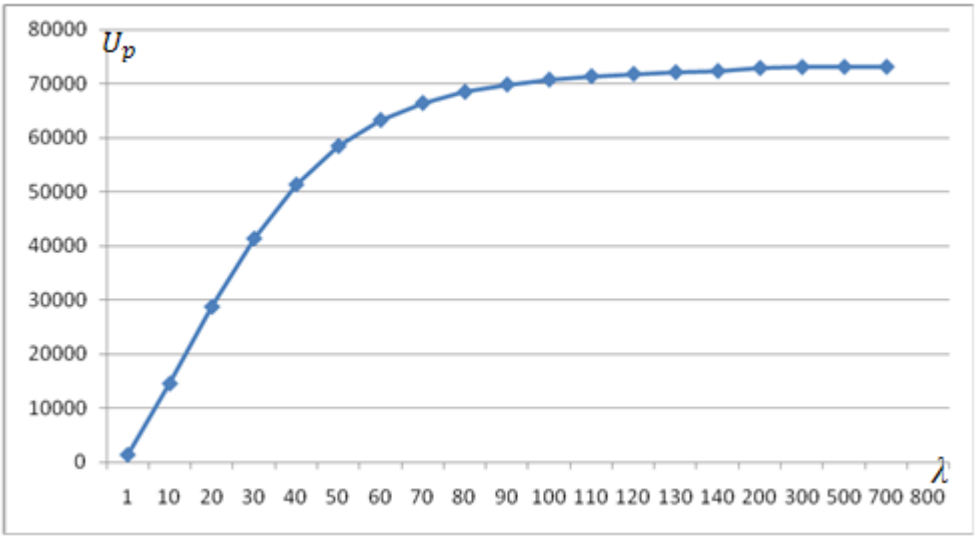


Рисунок 3.7 – График зависимости величины раскрытого потенциала от изменения параметра интенсивности действий злоумышленника λ.

Из приведенных графиков видно, что резкий скачок (в случае изменения λ) (рис. 3.7) и резкое снижение (в случае изменения μ) (Рисунок 3.6) происходит через определенный интервал (в этом случае, от 0 до 150). Это свойство было найдено во время различных экспериментов. Для объяснения этого факта необходимо рассмотреть модель физического компонента. Параметр λ характеризует число успешных переходов нападающего из одной подсистемы в другую динамик, а параметр μ - число вынужденных переходов к предыдущему акустической подсистемы, в связи с невозможностью НРД.

Из приведенных графиков видно, что резкий скачок (в случае изменения λ) (рис. 3.7) и резкое снижение (в случае изменения μ) (Рисунок 3.6) происходит через определенный интервал (в этом случае, от 0 до 150). Это свойство было найдено во время различных экспериментов. Для объяснения этого факта необходимо рассмотреть модель физического компонента. Параметр λ характеризует число успешных переходов нападающего из одной подсистемы в другую динамик, а параметр μ - число вынужденных переходов к предыдущему акустической подсистемы, в связи с невозможностью саботаже

3.3 Расчет времени передачи пакетной информации

Время передачи (обслуживания) μ при обслуживании пакетов, является величиной постоянной и определяется

$$\mu = t_{обсл} = (L_и + L_{сл})/R_k \qquad (3.5)$$

где $L_и$ – длина информационной части пакета, бит;

$L_{сл}$ – служебные биты (преамбула и концевик) пакета, бит;

R_k – пропускная способность тракта между маршрутизаторами, бит/с;

$t_{обсл}$ – время обслуживания;

μ – время передачи.

$$\mu = t_{обс} = \frac{(40 \cdot 1024 + 300)}{2048 \cdot 1024} = 0.02 \text{ с}$$

Коэффициент использования $К_{исп}$, который находится по формуле

$$K_{исп} = \frac{mR_и}{2R_к}\left(1 + \frac{L_{сл}}{L_и}\right) \quad (3.6)$$

где m – число абонентов, установивших связь с выходным маршрутизатором;

$R_и$ – скорость передачи данных от терминала, бит/с.

$$K_{исп} = \frac{8 \cdot 16 \cdot 1024}{2 \cdot 2048 \cdot 1024} \cdot \left[1 + \frac{300}{40 \cdot 1024}\right] = 0{,}031$$

Среднее время запаздывания m(T) имеет вид

$$m(t) = \frac{2 - K_{исп} - \frac{x}{1 - p + 2x}}{2 \cdot (1 - K_{исп})} \cdot \mu \quad (3.7)$$

Подставив значения в формулу (3.7) получим

$$m(t) = \frac{2 - 0{,}0.31 - \frac{0{,}3}{1 - 0{,}9 + 2 \cdot 0{,}3}}{2 \cdot (1 - 0{,}031)} \cdot 0{,}02 = 0{,}016$$

Типичные значения для вероятностей переходов являются P = 0,9 и x = 0,3, что соответствует случаю, когда 60% от временных рядов в состоянии 2 (обоих абонентов молчат) или 3 (сказал один из источников), то есть канал используется только на 40%.

Оценка средней задержки:

- при постоянных прибытия пакетов (M/D/1 модель) может быть определена по формуле

$$m(T) = \frac{0{,}75 - \frac{K_{исп}}{2}}{1 - K_{исп}} \mu$$

(3.8)

Подставив значения в формулу (3.8) получим

$$m(T) = \frac{0{,}75 - \frac{0{,}031}{2}}{1 - 0{,}031} \cdot 0{,}02 = 0{,}015 \text{ с}$$

– при поступлении пакетов по закону Пуассона (модель M/M/1)

$$m(t) = \frac{1 - \frac{K_{исп}}{2}}{1 - K_{исп}} \cdot \frac{L_{полн}}{R_и} \qquad (3.9)$$

$L_{полн}$ = 40·1024 + 300=41260 бит

$$m(t) = \frac{1 - \frac{0{,}031}{2}}{1 - 0{,}031} \cdot \frac{41260}{16 \cdot 1024} = 2{,}559 \text{ с}$$

– при поступлении пакетов по геометрическому закону (модель M/G/1)

$$m(t) = \frac{0{,}75 - \frac{K_{исп}}{2}}{1 - K_{исп}} \cdot \frac{L_{полн}}{R_и} \qquad (3.10)$$

$$m(t) = \frac{0.75 - \frac{0.031}{2}}{1 - 0.031} \cdot \frac{41260}{16 \cdot 1024} = 1.909 \text{ с}$$

Для оценки качества передачи речи в сети необходимо знать общую задержку, которая является суммой среднего задержки массового обслуживания и задержки задержки пакетирования кодека.

В результате задержка м (Т □) состоит из задержки в очереди т (Т), задержки пакетирования □ с и алгоритмической задержки □ кодера в кодере.

$$\delta_з = (L_и + L_{сл})/R_и, \qquad (3.11)$$

$$\delta_з = \frac{41260}{16 \cdot 1024} = 2.518$$

$$m(T_\Sigma) = m(T) + \delta_з + \delta_{кодер} = m(T) + (L_и + L_{сл})/R_и + \delta_{кодер} \qquad (3.12)$$

$m(T_\Sigma)$=0,015+2,518+5·10^{-3}=2,538 с

3.4 Выводы

Реализация и исследование математических моделей для оценки ущерба конфиденциальную информацию от внешних угроз показывает, что:

- Результаты моделирования были проанализированы в отношении влияния входных параметров.
- Чем выше техническое оснащение нападающего, тем выше риск несанкционированного доступа и, как следствие, тем выше повреждение.
- Увеличение параметра интенсивности λ злоумышленника НСД вероятности увеличивается, что в свою очередь тесно приближается к 100%. Соответственно, увеличение интенсивности параметра злоумышленник μ уменьшает вероятность несанкционированного доступа и тем быстрее, чем больше разница между λ и μ.
- Математическая модель гибко реагирует на изменения входных данных. Выявленные модели поведения модели для различных значений входных параметров.
- Математическая модель учитывает только небольшое число факторов. С одной стороны их количество достаточно, чтобы описать суть проблемы и понять общую структуру функционирования модели, с другой - для полного анализа проблемы необходимо учитывать, как много параметров, которые приведут к как увеличение сложности моделирования и точного результата.
- значения входных параметров.
- Математическая модель учитывает только небольшое число факторов. С одной стороны их количество достаточно, чтобы описать суть проблемы и понять общую структуру функционирования модели, с другой - для полного анализа проблемы необходимо учитывать, как много параметров, которые приведут к как увеличение сложности моделирования и точного результата.

4. Безопасность жизнедеятельности

4.1. Анализ опасных и вредных факторов, возникающих на рабочем месте пользователя ПЭВМ

Операторы ПК, программисты столкнулись с воздействием таких физически опасных и вредных факторов, таких как повышенный шум, бедных микроклиматических параметров, отсутствие или недостаток естественного света, низкая освещенность рабочей зоны, возможность поражения электрическим током, воздействия статического электричества и электромагнитное излучение. Также влияют физиологические факторы: психическое напряжение, перенапряжение зрительных и слуховых органов, монотонность труда, эмоциональные перегрузки.

Влияние этих негативных факторов приводит к снижению эффективности, усталости и раздражения, боли и недомогание.

Рассмотрим основные опасности:

Чтобы избежать искусственно низкой освещенности внутреннего освещения с источниками ПК люминесцентных предусмотренных в светильники. Величина света с искусственным светом в горизонтальной плоскости будет не менее 300 лк. Местные рабочем месте светильники операторы обеспечивается, монтируется непосредственно на рабочем столе. Они должны были не рассматривается отражатели и помещены ниже или на уровне линии оператора зрения, так, чтобы не вызвать блики.

В номерах, оборудованных ПК, статические токи электроэнергии чаще всего происходят, когда вы касаетесь любого из ПК сотрудников. Такое разряды опасности для людей нет, но кроме дискомфорта может привести к выходу оборудования из строя.

Для профилактики и защиты от статического электричества в помещении используется преобразователи и увлажнители воздуха, и полы антистатические покрытия, как антистатический ПВХ линолеума АСН.

Шум Исследование рабочем месте системы вентиляции создает компьютер и принтер. Уровень шума, создаваемого системой вентиляции, находится примерно в 40 дБА. В рабочее время, принтер переключается при необходимости, таким образом, шум должен быть классифицирован как непостоянным, с перерывами.

Для уменьшения шума в компьютерах номеров, принтеры установлены на амортизирующими подушками (резина). Уровни звука и эквивалентные уровни звука в комнате, где операторы работают ПК, не должно превышать 65 дБ.

Создание визуального отображения несколько типов излучения, в том числе рентген, радиочастоты, видимого и ультрафиолетового. Тем не менее, уровни этих выбросов являются довольно низкими и не превышают

действующие нормы.

Недостаточной чистоты и количество воздуха, необходимого. Основная цель систем кондиционирования воздуха является поддержание параметров воздуха в приемлемых пределах, чтобы обеспечить надежную работу ПК и комфортных условий для операторов.

Воздух должен быть очищен от пыли, а пыль оседает на устройства и ПК узлов, ухудшается теплообмен, могут образовывать проводящую цепь, в результате чего размытие движущихся частей и недопонимания.

При длительном применении части экрана, операторы отмечены штамма зрительного аппарата, возникают болезненные ощущения в глазах и боли в спине, головные боли, усталость.

Это приводит к нарушение сна, раздражительность, чувстве неудовлетворенности и т.д.

Чтобы предотвратить эти проявления сотрудников в рабочее время должны выполнять сложные гимнастические. Должны быть предусмотрены Каждые два часа работы перерывы на 10-15 минут.

Это Диссертация посвящена разработке моделей для оценки ущерба конфиденциальной информации от внешних угроз на кафедре информационной безопасности.

В области рабочего помещения от 6 х 6 м и высотой 3,5 м четыре ПК и две печатающие устройства, три настольные для разработчиков программного обеспечения, два вспомогательных таблиц, сейф дискет и другого вспомогательного оборудования, необходимого при работе с ПК, шкаф.

Площадь под основное и вспомогательное оборудование является 10,85 кв.м.

Общая площадь помещения составляет 36 кв.м. Рассчитаем площадь, приходящуюся на одного человека по формуле:

$$S_{чел} = S_{помещ} - S_{уст.обор}/N, \qquad (4.1)$$

где $S_{уст.обор}$ – площадь установленного оборудования,
$S_{помещ}$ – площадь помещения,
N – количество работающих в помещении человек.
$S_{чел} = 36 - 10{,}85/4 = 6{,}29$ кВ.м.

Т а б л и ц а 4.1 - Площадь под основное и вспомогательное оборудование

Оборудование	Количество	Размеры, мм	Площадь, $м^2$	Объем, $м^3$
Рабочий стол	4	1200*900*725	4,32	3,13
Вспомогательный стол	3	1000*600*725	1,80	1,31
Стул	4	450*450*800	0,81	0,65
Шкаф	1	3000*800*2000	2,40	4,80
Сейф	1	700*400*1500	0,28	0,42
Силовой щит	1	200*100*400	0,02	0,01
Системный блок	4	200*450*350	0,36	0,13
Монитор	4	350*450*350	0,63	0,22
Принтер	2	450*250*100	0,23	0,02
Итого			10,85	10,68

Это удовлетворяет нормы СанПиН, предусматривающий не менее 6 м от оборудования бесплатно площади на одного человека.

Высота помещения 3,5 м Расчет комнате для одного человека, рассчитывается по аналогичной формуле

$$V_{чел} = V_{помещ} - V_{уст.обор} / N, \qquad (4.2)$$

где $V_{уст.обор}$ – объем установленного оборудования,

$V_{помещ}$ – объем помещения,

N – количество работающих в помещении человек.

$V_{чел} = 126 – 10,68/4 = 28,83$ куб.м.

Это удовлетворяет нормы СанПиН, обеспечивая не менее 20 м3 свободного объема на человека.

Микроклимат и вентиляция бизнес. Под микроклиматические условия производственных мощностей понять состояние температуры, относительной влажности, скорости движения воздуха. Эти параметры имеют огромное влияние на функциональную активность человека и его здоровья и надежности компьютерной техники. Эти микроклиматические параметры влияют как индивидуально, так и в различных сочетаниях.

Для того чтобы создать нормальные условия для использования вычислительных зал персонал стандартам рабочей среды (СанПиН) для категории работ 1б. По этим стандартам установить значения температуры, относительной влажности и скорости движения воздуха для рабочей зоны комнате с ПК, которые представлены в таблице 4.2. В компьютерном зале используется воды системы центрального отопления. Следует обеспечить адекватное, непрерывный и равномерный нагрев воздуха в помещении в холодное время года.

Т а б л и ц а 4.2 – Микроклиматические условия

Период года	Температура воздуха, град. С не более	Относит. влажность воздуха, %	Скорость движения воздуха, м/с
	оптимальная	оптимальная	Оптимальная
Холодный	21 - 23	40 - 60	0,1
Теплый	22 - 24	40 - 60	0,1

Микроклимат влияние источников тепла, в районах с ПК. Для обеспечения установленных норм микроклиматических параметров и вентиляции чистый воздух и кондиционер используется. Расчет воздуха осуществляется с помощью избыточного тепла от ПК и вспомогательного оборудования, людей, солнечной радиации и искусственного освещения. Расчет производится для теплого времени года.

$$L = \frac{Q_{изб}}{c \cdot \rho \cdot (t_{вытяж} - t_{приточ})}, \quad (4.3)$$

где L – объем приточного воздуха, м^3/ч;

$Q_{изб}$ – избыточные тепловыделения, кДж/ч;

c – теплоемкость воздуха (1,005 кДж/(кг*^{O} С));

ρ – плотность приточного воздуха, кг/м^3, (ρ=1,2 кг/м^3);

$t_{вытяж}$, $t_{приточ}$ – температура вытяжного и приточного воздуха, ^{O}С.

Теплоизбытки в машинном зале можно определить по формуле

$$Q_{изб} = Q_{обор} + Q_{людей} + Q_{осв} + Q_{рад}, \quad (4.4)$$

где $Q_{обор}$ – выделение тепла от оборудования,

$Q_{людей}$ – поступление тепла от людей,

$Q_{осв}$ – выделение тепла от электрического освещения,

$Q_{ра}$ – поступление тепла от солнечной радиации,

Рассмотрим определение отдельных компонентов избыточного тепла в машинном отделении.

Теплота оборудования, которое потребляет электроэнергию:

$$Q_{обор} = 3600 \cdot N \cdot j_1 \cdot j_2, \quad (4.5)$$

где N – суммарная установленная мощность оборудования, кВт;

j_1 – коэффициент использования установочной мощности (j_1=0,95);

j_2– коэффициент одновременности работы (j_2= 0,8).

$$N = 3 \cdot N_{ЭВМ} + 2 \cdot N_{ПРН}, \quad (4.6)$$

где $N_{ЭВМ}$ – установочная мощность одной ЭВМ;

$N_{ПРН}$ – мощность печатающего устройства.

$N = 3 \cdot 0{,}25 + 2 \cdot 0{,}05 = 0{,}85$ кВт

Выделение тепла от людей

$$Q_{людей} = n \cdot q \qquad (4.7)$$

где *n* – количество людей, одновременно работающих в машинном зале;

q – количество тепла, выделяемого одним человеком (для категории работ на *q* = 150 ккал/ч = 4,1868 · 150 = 628,02 Дж/ч).

$Q_{людей} = 4 \cdot 628{,}02 = 2512{,}08$ (кДж/ч)

Поступление тепла от электрического освещения

$$Q_{осв} = 3600 \cdot N \cdot n \cdot k_1 \cdot k_2, \qquad (4.8)$$

где *N* – мощность одной лампы, кВт;

n – количество ламп.

k_1, k_2 – коэффициенты, учитывающие способ установки и особенности светильников (для встроенных в подвесной потолок светильников с люминесцентными лампами $k_1 = 0{,}3$; $k_2 = 1{,}3$).

$Q_{осв} = 3600 \cdot 0{,}04 \cdot 16 \cdot 0{,}3 \cdot 1{,}3 = 898{,}56$ (кДж/ч)

Количество тепла, поступающее от солнечной радиации

$$Q_{рад} = q' \cdot F \cdot C + F \cdot \frac{t_н - t_в}{R}, \qquad (4.9)$$

где *q'* – поступление тепла при наклонном заполнении светового проема, облучаемого прямой солнечной радиацией, ккал/м^2·ч,

F – суммарная площадь окон в помещении;

C – коэффициент относительного проникновения солнечной радиации (*C*=0,59 для окон со средними по окраске шторами);

$t_н$, $t_в$ – температура наружная и внутренняя;

R – сопротивление теплопередачи, ч·м^2·^{O}С/ккал (*R*=0,4 для окон со шторами);

Второе слагаемое в правой части формулы для вентиляции с испарительным охлаждением не учитывается.

$$q' = q_{г.п.} \cdot K_3 \cdot q_{в.п.} \cdot K_4 + q_{г.р.} \cdot K_1 \cdot K_2, \qquad (4.10)$$

где K_1 – коэффициент, учитывающий затенение остекления световых проемов переплетами и загрязнение атмосферы (K_1=0,9);

K_2 – коэффициент, учитывающий загрязнение стекла (K_2=0,95); $q_{г.п.}$ и $q_{в.п.}$ – количество тепла прямой солнечной радиации в июле на широте

45 градусов, поступающего в помещение через окна соответственно горизонтального и вертикального заполнения светового проема, ккал/ч·м^2;

$q_{г.р.}$ – количество тепла рассеянной солнечной радиации в июле на широте 45 градусов, поступающего в помещение через окна горизонтального заполнения светового проема, ккал/ч·м^2.

Значения этих параметров возьмем максимальными из возможных в течение рабочего дня: ≈ 360 ккал/ч·м^2 ≈ 100 ккал/ч·м^2 (оба окна ориентированы на запад).

Значения коэффициентов $К_3$ и $К_4$ при угле наклона плоскости окна к горизонту 90° соответственно равны 0 и 1.

$q' = (360 + 100)$ккал/м^2 · ч = 1925,28 кДж/м^2·ч,

Площадь окон вычисляется с учетом неизбежной установки кондиционеров

F = 2 · 2,3 · 1,8 – 0,306 · 3 = 7,362м^2,

$Q_{рад}$= 1925,28 · 7,362 · 0,59 = 8361,39 кДж/ч,

В ориентировочных расчетах вентиляции можно принять

t = 28 - 18 = 10 (^{o}C) Найдем количество приточного воздуха

$$L = \frac{Q_{изб}}{c \cdot \rho \cdot (t_{вытяж} - t_{приток})} = \frac{13469,61}{1,005 \cdot 1,2 \cdot 10} = 1116,88 \text{ (м}^3\text{/ч)}$$

Подача воздуха в помещение предполагается использовать тип кондиционера ВС-2500, который имеет размеры 460 х 660 х 615 мм, способной подавать объем воздуха 620 м3 / ч Кондиционер обеспечивает разницу температур в 10 градусов.

Необходимое количество кондиционеров

$$n = \frac{L}{V}, \qquad (4.11)$$

где V – производительность кондиционера.

n = 1116,88 / 620 = 1,8.

Округляем результат до целого числа: n = 2.

Таким образом, для создания благоприятных условий в выбранной комнате кондиционер должен быть типа 2 ВС-2500, которые устанавливаются в оконных рамах.

Таким образом, чтобы обеспечить необходимую климат в помещении и отвечают санитарным нормам достаточно оборудованные офисные помещения только с двумя кондиционерами отечественного производства.

Конечно, соблюдать санитарные нормы должны также минимизировать влияние других вредных факторов.

4.2 Расчет искусственного освещения

Для расчета общего равномерного освещения горизонтальных поверхностей при отсутствии крупных объектов с использованием затенения использование метода.

Исходные данные для помещения

– ширина B = 6м;

– длина A =6м;

– высота H = 3,5м.

Чтобы обеспечить необходимую освещенность комнаты с параметрами 6x6x3, 5 м необходимо установить 4 типа лампы типа люминесцентная лампа LSP 22-65-002, 65 Вт, световой поток 3570 лм, диаметр 94 мм и длиной 1225 мм, с булавки. Они имеют длительный срок службы (до 14000 часов) и оптимальный световой поток. Их использование никаких визуальных анализаторов усталость не вызывает функциональные расстройства глаза.

Необходимое количество N, светильники

$$N = \frac{E \cdot K_З \cdot S \cdot Z}{n \cdot Ф_Л \cdot \eta}, \quad (4.12)$$

где E – заданная минимальная освещенность, для помещения, (E=300 лк);

$K_з$ – коэффициент запаса, при искусственном освещении газоразрядными лампами в автозале, $K_з$ = 1,5;

S – освещаемая площадь, м^2;

Z – коэффициент неравномерности освещения Z = 1,1 ÷ 1,2;

n – количество ламп в светильнике, равно еденице;

$Ф_л$ – световой поток, для ламп типа ЛД номинальной мощностью 65 Вт, $Ф_л$ = 3570 лм;

η - коэффициент использования;

Чтобы обеспечить необходимую освещенность комнаты с параметрами 6x6x3, 5 м необходимо установить 4 типа лампы типа люминесцентная лампа LSP 22-65-002, 65 Вт, световой поток 3570 лм, диаметр 94 мм и длиной 1225 мм, с булавки. Они имеют длительный срок службы (до 14000 часов) и оптимальный световой поток. Их использование никаких визуальных анализаторов усталость не вызывает функциональные расстройства глаза.

Необходимое количество N, светильники

Индекс помещения i определяется

$$i = \frac{A \cdot B}{h \cdot (A+B)}, \quad (4.13)$$

где A – длина помещения, м;

B – ширина помещения, м;

h - расчетная высота, h = 3,5-0,7=2,8 Подставим данные в формулу

i = 6 · 6 / 2,8 · (6+6) = 1,071

Коэффициент использования η = 60%.

Подставляя в формулу все значения, определим количество люминесцентных ламп.

N = 300 · 1,5 · 36 · 1,2 / 2 · 3570 · 0,6 = 4 шт

Найдем расстояния между светильниками, учитывая λ=0,6÷2,0.

$$L_A=\lambda \cdot h_p, \quad (4.14)$$

L_A =1,3·2,8=4 м

$$L_B=\lambda \cdot h_p, \quad (4.15)$$

L_B=0,7·2,8=2 м

l_a =0,5·4=2 м

l_b =0,5·2=1 м

Схема расположения светильников в помещении показана на рисунке 4.1.

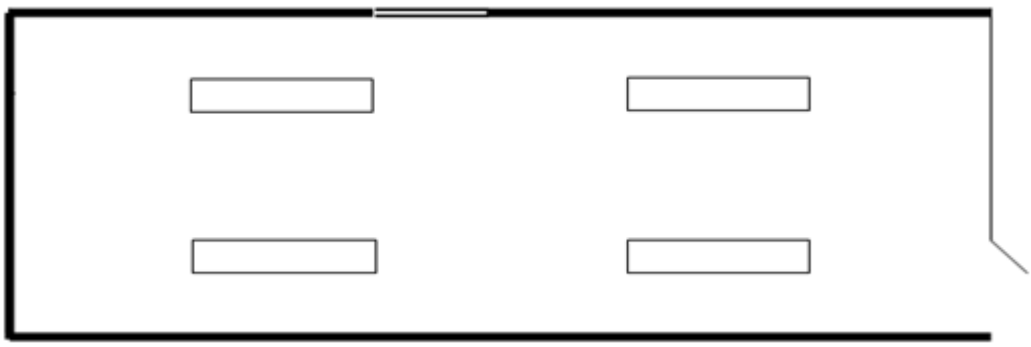


Рисунок 4.1 - Размещение светильников в помещении

4.3 Выводы

1. Показали основные негативные факторы, влияющие на компьютер пользователя во время работы.

2. Рассчитано систему для поддержания постоянного микроклимата в помещениях для работы на компьютере.

3. Испытано на соответствие санитарным нормам помещений для работы на компьютере.

4. Параметры системы кондиционирования воздуха в комнате для обеспечения комфортной работы.

1. Бизнес план

5.1. Общая информация о проекте

Место реализации проекта: Филиал ОАО «InfoWatch» «Технический центр" в Алматы.

Основными видами деятельности филиала в Алматы являются:

- защита конфиденциальной информации;
- исследование информационных инцидентов;
- управление рисками;
- управление корпоративной репутацией;

InfoWatch Группа объединяет ряд разработчиков программного обеспечения и решений для организации информационной безопасности, противодействия внешним и внутренним угрозам.

InfoWatch решения современные средства управления рисками, связанными с потерей ценной информации, а также в качестве инструмента для анализа и бизнес-аналитики (BusinessIntelligence), включая мониторинг работы персонала и степени лояльности к компании.

Рынок по-прежнему ждет единую комплексную автоматизированную систему управления рисками, которая учитывает все возможные аспекты - политические, организационные, правовые, экономические, финансовые, репутационные, рынок, информационных, и многие другие. Но нет такого решения, поэтому управляющие компании должны сами принять все меры по минимизации рисков, которые могут негативно отразиться на бизнес.

Тривиальной задачей, и трудно без специализированных систем разрешимых. Для упрощения этой задачи может помочь инструменты, которые используют, чтобы решить проблему Riskmanagement на первый взгляд не столь очевидно.

Правильно состоит матрица рисков - риск - Нарушитель - Решение поможет минимизировать риски точно предсказать стоимость и планировать задачи в рамках всей организации.

InfoWatch решения можно обнаружить и минимизировать стратегические, оперативные, репутационные и юридические риски. А именно

а) стратегические риски

1) защита интеллектуальной собственности и коммерческой тайны;

2) защита персональных данных клиентов (клиентские базы);

3) Защита от утечек секретной и бизнес-информации;

4) предотвращение уничтожения ценной информации;

5) предотвращение мошенничества, возможность расследовать инцидент и выявить лиц, причастных;

6) контроль за имидж бренда компании.

б) репутационные риски:

1) для предотвращения утечки конфиденциальных данных;

2) предотвратить распространение негатива внутри компании и за ее пределами;

3) выявление информации "вброс бюллетеней" негативный или ущерба природе («черный пиар»);

4) определение нелояльных сотрудников.

Защита конфиденциальной информации - задача столь же как технических, так и правовых, и организационных. Только после формируется правильное понимание ", что защищать", а кто в компании должен четко установить цели и задачи, вы можете начать внедрение систем информационной безопасности.

В результате внедрения и использования InfoWatch решений компании получает уверенность в безопасности ценных и конфиденциальных данных, знаний и систематическое понимание всех внутренних и внешних информационных потоков организации, сокращения бизнес-рисков, а также:

- аудит и оптимизация состояния информационной безопасности в компании, в результате чего информационную структуру в соответствие с нормативными требованиями;

- классификация информационных ресурсов и идентификации информационных ресурсов;

- создана коммерческая тайна, которая полностью соответствует закону и правовыми актами Республики Казахстан;

- юридически хорошо написаны «Положение о коммерческой тайне" и связанных с ним документов, которые сведут к минимуму юридические риски в случае инцидентов в области безопасности и позволяют судебного преследования виновного лица.

5.2. Финансовый план

5.2.1 Расчет капитальных вложений. Затраты по капитальным вложениям на реализацию проекта включают в себя затраты на приобретение основного оборудования, монтаж оборудования, транспортные расходы и проектирование, и рассчитывается по формуле

$$\Sigma К = Ко + Ку + Кз\text{-}с + Ктр + Куп, \qquad (5.1)$$

где Ко – капитальные вложения на приобретение оборудования;

Км - расходы по монтажу оборудования;

Ктр- капитальные вложения на транспортные расходы;

Кпр - затраты на проектирование.

Общий перечень необходимого основного оборудования и его стоимость приведены в таблице 5.2.

Таблица 5.2 - Смета затрат на приобретение основного оборудования для реализации проекта «Модель оценки ущерба конфиденциальной информации от внешних угроз»

Наименование	Количество, шт.	Цена за ед., тенге	Сумма, тенге (без НДС)
СерверHP ProLiant ML350p Gen8 Series	1 шт	478 610	478 610
Коммутатор Cisco SF200-24P	1 шт	68 500	68 500
Компьютер DEL1H615232	4шт	139 890	559 560
Монитор Samsung S22B300BS	5 шт	32 510	162 550
Маршрутизатор 4-port TL-WDR4300 Router Tp-Link	1 шт	17 910	17 910
МФУНр LaserJet Pro M1536dnf	2шт	49 910	99 820
Кабельная продукция UTP 5e	100 м	40	4 000
Прочие материалы			200000
ИТОГО:	1 587 350		

Транспортные расходы, составляют 3 % от стоимости всего оборудования.
Монтаж оборудования, пуско-наладка производится инженерами-монтажниками, расходы составляют 1% от стоимости всего оборудования и рассчитываются по формуле

$$Км = 0{,}01 \cdot Ко, \qquad (5.2)$$

Км = 0,01 · 1 587 350 = 15873 тенге

Расходы по проектированию и разработке проекта составляют 0,5% от стоимости всего оборудования

Общая сумма капитальных вложений по реализации проекта составляет

ΣК = 1 587 350 + 47 620 + 15 873 + 7 936 = 1 658 779 тенге

5.2.2 Эксплуатационные расходы. Текущие затраты на эксплуатацию данной системы связи определяются по формуле:

$$ΣЭ = ФОТ + O + Э + А + З_н, \qquad (5.3)$$

где ФОТ – фонд оплаты труда;

О – отчисления на соц. нужды;

А – амортизационные отчисления;

Э – электроэнергия для производственных нужд;

$З_н$ – накладные затраты.

Фонд оплаты труда. В штате данного проекта состоят 7 человек:
Заработная плата сотрудников приведена в таблице 5.3

Т а б л и ц а 5 . 3 – Заработная плата сотрудников

Должность	Количество	Оклад, тг.	Сумма з/п, тг.
главный специалист	1	300 000	300 000
инженер - электрик	1	140 000	140 000
ведущий инженер	1	250 000	250 000
инженер 1 уровня	4	200 000	800 000
итого	7		1 490 000

Величину общего годового фонда оплаты труда ($ФОТ_г$) можно рассчитать по формуле:

$$ФОТ_г = ФЗП \cdot N_м \cdot Пр \cdot К_{вр}, \quad (5.4)$$

где $ФЗП$ – основной фонд заработной платы, $ФЗП$ = 360000 тенге;

$N_м$ – количество месяцев в году, $N_м$ = 12;

$Пр$ – размер премии, $Пр$ = 1,25 (25%);

$К_{вр}$ – коэффициент, учитывающий доплату за работу с вредными условиями труда, $К_{вр}$ = 1,04.

$ФОТ_г$ = 1 490 000 · 12 · 1,25 · 1,04 = 23 244 000 тенге

Отчисления в социальный налог берутся в размере 11% от фонда оплаты труда.

$$О=0,11\cdot(ФОТ_г – 0,1 \cdot ФОТ_г), \quad (5.5)$$

О = 0,11·(23 244 000 – 0,1·23 244 000) = 2 301 156 тенге

Расчет затрат на амортизацию.

Амортизационные отчисления берутся исходя из того, что норма амортизации на оборудование связи составляет 25 % и вычисляются по следующей формуле

$$А = К_{осн.i} \cdot Н_{а.i}, \quad (5.5)$$

где $К_{осн.i}$ – первоначальная стоимость основных фондов ($К_{осн.i}$ приравнивается к капитальным вложениям);

$Н_{а.i}$ – норма амортизационных отчислений основных фондов, $Н_{а.i}$ = 25%.

Тогда амортизационные отчисления составляют:

$А$ = 1 587 350·0,25 = 396 837 тенге

Расчет на материальных затрат. Материальные затраты для производственных нужд в течение года, включают в себя расходы

электроэнергии на оборудование и дополнительные нужды и рассчитываются по формуле

$$М_з = З_{эн} + З_м, \quad (5.6)$$

где $З_{эн}$ – затраты на оплату электроэнергии;

$З_м$ – затраты на материалы и запасные части.

Затраты электроэнергии на оборудование рассчитывается по формуле

$$З_{эн} = Т \cdot 30 \cdot 365 \cdot Р, \quad (5.7)$$

где $Т$ – тариф на электроэнергию, Т = 22,79 тг./кВт/час;

$Р$ – мощность оборудования, для eNB $Р$ = 1,075 кВт.

$З_{эн}$ = 22,79 · 24 · 365 · 1,075 = 241 613 тенге

Затраты на дополнительные нужды составляют 5% от затрат на оборудование и рассчитываются по формуле

$$З_м = К \cdot 0,05, \quad (5.8)$$

$З_м$ = 1 587 350·0,05 = 79 367 тенге

Тогда суммарные затраты на электроэнергию будут равны

$М_з$ = 241 613 + 79 367 = 320 980 тенге

Другие расходы включают в себя общее производство, рабочие и деловые расходы, ремонт и обслуживание зданий, некоторые налоги, страхование имущества, расходы на рекламу, аудит и гостеприимство. Прочие расходы рассчитываются следующим образом:

$$З_{пр} = 0,4 \cdot ФОТ, \quad (5.9)$$

$З_{пр}$ = 0,4 · 23 244 000 = 9 297 600 тенге

Т а б л и ц а 5 . 4 – Годовые эксплуатационные расходы

Показатель	Сумма тенге
ФОТ	23 244 000
Отчисления на социальные нужды (Ос)	2 301 156
Амортизационные отчисления ($А_0$)	396 837
Материальные затраты ($М_з$)	320 980
Прочие расходы ($З_{пр}$)	9 297 600
ИТОГО	3 556 0573

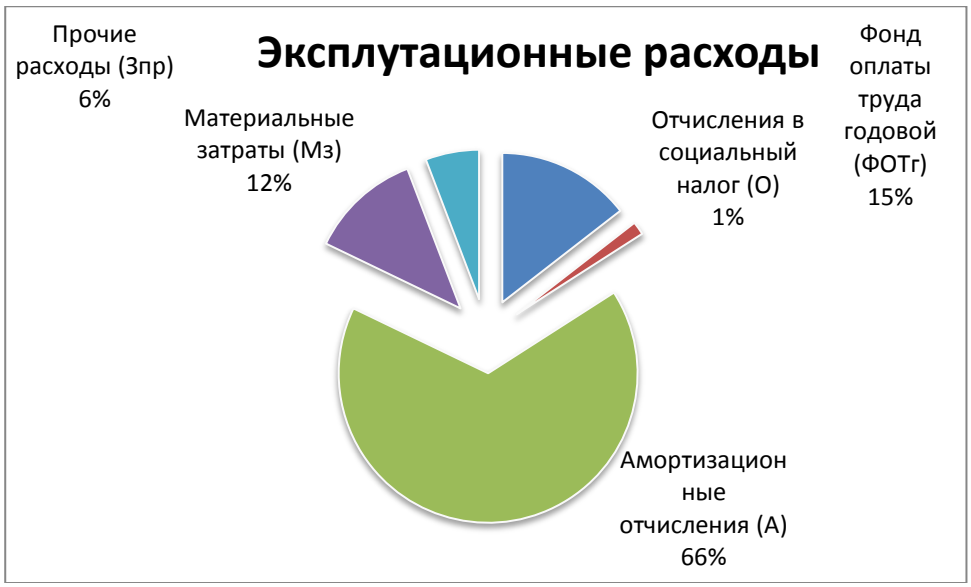


Рисунок 6.1 - Диаграмма эксплуатационных затрат

Затраты на эксплуатацию данной системы связи определяются по формуле 5.3

ΣЭ = 23 244 000 + 2 301 156 +396 837 + 320 980 + 9 297 600 = 35 560 573 тенге

5.3.3 Расчет доходов от внедрения системы. Реальный доход, получаемый от полного внедрения системы можно определить по следующей формуле

.

$$Д = Д_{под} \cdot Д_{обс} \cdot Д_{обн}, \quad (5.15)$$

где $Д_{под}$ – доход от подключения пользователей в год;

$Д_{обс}$ – доход от обслуживания системы в год

$Д_{обн}$ – доход от обновления ПО.

Доходы от платежей за подключение в год рассчитывается по формуле

$$Д_{под} = T \cdot N \cdot 12, \quad (5.16)$$

где T – тариф за подключение равен 2500 тенге (1 месяц);

N – количество новых пользователей (берется приблизительно исходя из статистических данных по г.Алматы).

Расчет доходов от платежей за подключение за 3 года

$Д_{под}$ = 2500 · 500 · 12 = 15 000 000 – 1 год

$Д_{под}$ = 2500 · 800 · 12 = 24 000 000 – 2 год

$Д_{под}$ = 2500 · 1000 · 12 = 30 000 000 – 3 год

Доход от обслуживания системы в год рассчитывается по формуле

$$Д_{обс} = N \cdot J \cdot 12, \quad (5.17)$$

где N – количество клиентов (берется приблизительно исходя из статистических данных по г.Алматы);

J – средняя цена за работу специалиста по обслуживанию системы.

Расчет доходов от платежей за обслуживание системы за 3 года

$Д_{под} = 1500 \cdot 500 \cdot 12 = 9\ 000\ 000$ – 1 год

$Д_{под} = 1500 \cdot 800 \cdot 12 = 14\ 000\ 000$ – 2 год

$Д_{под} = 1500 \cdot 1000 \cdot 12 = 18\ 000\ 000$ – 3 год

Доход от услуги обновления ПО в год рассчитывается по формуле

$$Д_{обн} = N \cdot Ф_{по} \cdot 12, \qquad (5.18)$$

где $Ф_{по}$ – средний тариф на обновление ПО.

N - количество абонентов пользующихся услугами системы (берется приблизительно исходя из статистических данных по г. Алматы).

Расчет доходов от обновления ПО за 3 года

$Д_{под} = 500 \cdot 500 \cdot 12 = 3\ 000\ 000$ – 1 год

$Д_{под} = 500 \cdot 800 \cdot 12 = 4\ 800\ 000$ – 2 год

$Д_{под} = 500 \cdot 1000 \cdot 12 = 6\ 000\ 000$ – 3 год

Результаты расчета доходов в результате внедрения проекта г. Алматы занесены в таблицу 5.5

Т а б л и ц а 5 . 5 –Таблица доходов от внедрения услуг связи по годам

Наименование показателя	1 год	2 год	3 год
Количество новых пользователей, в ед.	500	800	1000
Разовый платеж за подключение, в тенге	3000	3000	3000
Доходы от подключения клиентов за год, в тенге	15 000 000	24 000 000	30 000 000
Доходы от обслуживания системы за год, в тенге	9 000 000	14 400 000	18 000 000
Расчет доходов от обновления ПО за год	3 000 000	4 800 000	6 000 000
Реальные доходы за год, в тенге	27 000 000	43 200 000	54 000 000

Оценка эффективности проекта «оценки ущерба Модель конфиденциальной информации от внешних угроз" базируется на следующих показателях:

- Чистый доход;
- Чистая приведенная стоимость;
- Срок окупаемости без дисконтирования;
- Срок окупаемости дисконтирование.

Для расчета срока окупаемости необходимо определить чистую прибыль и доход компании после уплаты налогов.

Чистый доход предприятия определим по формуле

$$Д_{чис} = Д – ΣЭ, \quad (5.19)$$

где Д - реальный доход от внедрения услуг в год;

ΣЭ – эксплуатационные расходы.

$Д_{чис}$ = 41 686 182 – 35 560 573 = 6 125 609

Сумма налога в бюджет составляет 20% от чистого дохода предприятия. Чистый доход предприятия после налогообложения рассчитывается по формуле

$$D_{ЧИСТ.Н.} = 0,8 \cdot Д_{чис}, \quad (5.20)$$

где $D_{ЧИСТ.Н.}$ – чистый доход предприятия.

Тогда чистый доход после налогообложения составит:

$D_{ЧИСТ.Н.}$ = 0,8 · 6 125 609 = 4 900 488 тенге

Рентабельность капиталовложений рассчитывается по формуле

$$E = \frac{Д-К}{К} = \frac{ЧП}{К}, \quad (5.20)$$

$$E = \frac{2\ 844\ 871}{1\ 658\ 779} = 1,7$$

Период окупаемости рассчитывается по формуле (5.21)

$$T = 1/E, \quad (5.21)$$

T = 1 / 1,7 = 0,58

Из расчета видно, что о прибылях и убытках зависит от количества клиентов, подключенных к системе. После 6 месяцев, когда компания начинает платить полностью, возможно, направление входящих средств на дальнейшее развитие системы и разработку более совершенных средств защиты информации, которые имеют непосредственное влияние на доходы предприятия.

5.4 Выводы по разделу «Бизнес план»

В этой части дипломного проекта был представлен разработанную систему бизнес-план с указанием на срок окупаемости проекта.

С финансовой точки зрения были рассчитаны объем инвестиций, равный 1658779 тенге, размер эксплуатационных расходов равными
35560573 тенге.

Указано Срок окупаемости (возврата) капитальных вложений характеризует период в годы, в течение которого инвестиции будут возвращены в полном

прибыль и составляет 5 лет, коэффициент сравнительной экономической эффективности ЕН = 0,2. Исходя из вышеприведенного финансово-экономического обоснования проекта, можно сделать вывод, что проект является экономически жизнеспособным и эффективным, так как рассчитывается срок окупаемости 7 месяцев и вернуться на инвестиционный Е=3

Таблица 5.7 – Показатели экономической эффективности проекта

Наименование	Показатель
Капитальные затраты, тенге	1 658 779
Текущие затраты, тенге	35 560 573
Доходы, тенге	6 125 609
Прибыль, тенге	4 900 487
Коэффициент экономической эффективности	1.7
Срок окупаемости, лет	0.58 (7месяцев)

Заключение

В данной дипломной работы были главными методов оценки ущерба: естественный эксперимент, ЛИХ, методы оценки эксперт, математическое моделирование. Все эти методы имеют как близкие, так плюсы и минусы. Но исследования в рамках этого тезиса был самый интересный метод математического моделирования. В результате, математическая модель была разработана на основе современной концепции вопросу. Для моделирования этого типа был использован прибор марковских процессов, которые в настоящее время широко используются в системах массового обслуживания, и анализируя действия злоумышленников.

В математического моделирования учитывает только определенное количество параметров, которые влияют на исход моделирования. Обычно выбирают только основные критические условия моделирования. Математическая модель также использует только самые важные и необходимые внешние параметры. С одной стороны, это можно упростить модель и больше внимания к структуре математической модели. С другой стороны, результаты являются приблизительными, и для получения более точных результатов необходимо использовать большее количество параметров (внешних и внутренних).

Разработанная модель позволяет адаптировать свои дополнения структуры и изменения, чтобы получить более точные результаты. Например, модель использует ряд постоянных значений, определение которых может быть осуществлено на своих собственных математических моделей. И, как было описано выше, более подробное определение этих параметров может повысить точность результатов, но это может увеличить сложность и полученный образец.

Список литературы

1 Белов, Е. Б. Основы информационной безопасности: учеб. пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М. : Горячая линия – Телеком, 2006. – 544 с.

2 Гришина, Н. В. Организация комплексной системы защиты информации [Текст] : учеб. пособие / Н. В. Гришина. – М. : Гелиос АРВ, 2007. – 256 с.

3 Бузов, Г. А. Защита от утечки информации по техническим каналам: учеб. пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия – Телеком, 2005. – 416 с.

4 Домарев, В. В. Безопасность информационных технологий. Методология создания систем защиты: учебное пособие / В. В. Домарев. – М. : ТИД «ДС», 2006. – 688 с.

5 Крысин, А. В. Информационная безопасность: практическое руководство / А. В. Крысин – М. : Спаррк, 2003. – 320 с.

6 Максимов, Ю. Н. Технические методы и средства защиты информации [Текст] : учебное пособие / Ю. Н. Максимов, В. Г. Сонников, В. Г. Петров. – СПб : Полигон, 2000. – 314 с.

7 Грушко, А. А. Теоретические основы компьютерной безопасности: учеб. пособие / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – М. : Академия, 2009. – 272 с.

8 Мельников В. В. Безопасность информации в автоматизированных системах: учебное пособие / В. В. Мельников. – М. : Финансы и статистика, 2003. – 368 с.

9 Михайлов, Г. А. Численное статистическое моделирование. Методы Монте-Карло: учебное пособие / Г. А. Михайлов, А. В. Войтишек. – М. : Академия, 2006. – 368 с.

10 Романец, Ю. В. Защита информации в компьютерных системах и сетях: учебное пособие / Ю. В. Романец, П. А. Тимофеев, В. Ф Шаньгин. – М. : Радио и связь, 2001. – 304 с.

11 Семкин, С. Н. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие / С. Н. Семкин, Э. В. Беляков, С. В. Гребенев , В. И. Козачок. – М. : Гелиос АРВ, 2005. – 192 с.

12 Чипига, А. Ф. Информационная безопасность автоматизированных систем: учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности / А. Ф. Чипига. – М. : Гелиос АРВ, 2010. – 336 с.

13 Шелухин, О. И. Моделирование информационных систем: учеб. пособие для студентов вузов / О. И. Шелухин. – М. : Горячая Линия - Телеком, 2011. – 536 с.

14 Ярочкин, В. И. Информационная безопасность: учебник для студентов вузов / В. И. Ярочник. – М. : Академический проект, 2004. – 544 с.

15 Чашкин, Ю. Р. Математическая статистика. Анализ и обработка данных: учеб. пособие для студентов вузов / Ю. Р. Чашкин. – Ростов н/Д. : Феникс, 2010. – 240 с.

16 Гмурман, В. Е. Теория вероятностей и математическая статистика: учеб. пособие для вузов / В. Е. Гмурман. – М. : Высшая школа, 2003. – 479 с.

17 СНиП 2.2.2.5.542-96. Гигиенические требования к видеодисплейным терминалам, персональным ЭВМ и организация работ.– Взамен Временных санитарных норм и правил для работников вычислительных центов ; Введ. 1996-07-14. – М. : Изд-во стандартов, 1996. – 19 с.

18 Маринченко А.В. Безопасность жизнедеятельности: Учебное пособие. – 2-е изд., доп. и перераб. – М.: Издательско-торговая корпорация «Дашков и К», 2007. – 106 с.

19 Абдимуратов Ж.С., Манабаева С.Е. Безопасность жизнедеятельности. Методические указания к выполнению раздела «Расчет производственного освещения» в выпускных работах для всех специальностей. Бакалавриат – Алматы: АИЭС, 2009.

20 Голубицкая Е.А., Жигуляская Г.М. Экономика связи. – М.: Радио и связь, 1999. – 142 с.

21 Анализатор сетевых протоколов Wireshark [Электронный ресурс]. — Режим доступа: http://www.wireshark.org.

22 Среднестатистический населенность пользователей г. Алматы – Режим доступа: http://www.zakon.kz/4495443-chislennost-naselenija-almaty.html

23 Спецификация протокола управления передачей данных (Transmission Control Protocol) [Электронный ресурс]. — Режим доступа: http://citforum.ru/nets/tcp/tcpspec.shtml.