Министерство образования Калининградской области
государственное автономное учреждение
Калининградской области
профессиональная образовательная организация
«Колледж предпринимательства»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ (ДИПЛОМНАЯ) РАБОТА

Тема: Защита локальной сети

Выпускная квалификационная
(дипломная) работа
допущена к защите
Заместитель директора по УМР

_____ Бурыкина Ю.И.
«___»_____2020 г.

Выполнил:
обучающийся группы КС 16-2
специальность 09.02.02
Компьютерные сети

_____Давыдов Т.А.

Руководитель:

_____Зверев М.В.

Калининград
2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ....3

1 АНАЛИЗ ПОТЕНЦИАЛЬНЫХ УГРОЗ ОПЕРАТИВНО-ТЕХНОЛОГИЧЕСКОЙ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ СЕТИ....8

1.1 Основные цели сетевой безопасности....8

1.2 Модели безопасности....13

1.3 Виды угроз и методы защиты....18

2 ПРОЕКТИРОВАНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЛОКАЛЬНОЙ СЕТИ....29

2.1 Понятие политики безопасности. Межсетевой экран как инструмент реализации политики безопасности....29

2.2 Особенности и преимущества предлагаемого решения. Разработка и коррекция правил политики безопасности....36

2.3 Методика построения корпоративной системы защиты информации....40

3 РЕАЛИЗАЦИЯ КОМПЛЕКСА МЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ СЕТИ....51

3.1 Информационная модель системы управления предприятием ООО «АйТиЭл»....51

3.2 Характеристика решаемых управленческих задач....55

3.3 Выбор и описание локальной компьютерной сети....57

3.4 Сетевое программное обеспечение ООО «АйТиЭл»....59

3.5 Пользовательское программное обеспечение. Построение схемы сети....60

4 АНАЛИЗ ЗАТРАТ НА ОРГАНИЗАЦИЮ И ОБСЛУЖИВАНИЕ ЛОКАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ И ЭФФЕКТИВНОСТИ СИСТЕМЫ БЕЗОПАСНОСТИ....62

ЗАКЛЮЧЕНИЕ....71

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ....77

ПРИЛОЖЕНИЯ....78

ВВЕДЕНИЕ

Любое государственное и коммерческое предприятие заинтересовано в сохранении информации, которая может ему навредить, если попадёт в руки злоумышленников или будет уничтожена. Для государственных учреждений такая информация носит гриф “Секретно”, для коммерческих предприятий — “Коммерческая тайна” или “Ценная информация”.

Зададимся вопросом: какая именно информация нуждается в защите и может представлять интерес для злоумышленника? Это, как правило, важные договоры, списки клиентов, базы данных бухгалтерских программ, пароли и ключи системы “клиент-банк”, каналы связи с подразделениями и т. п.

Всё чаще в СМИ сообщают о краже информации и денежных средств через интернет, при этом хакера находят очень редко. А большинство предприятий скрывают случаи взлома своих сетей и кражи данных, чтобы сохранить деловую репутацию.

Чтобы не стать жертвой хакера, необходимо защищать компьютеры и всю сеть организации от интернет-угроз. И не стоит утешать себя тем, что, мол, именно ваше предприятие не заинтересует злоумышленника: ведь специальные программы — сканеры уязвимостей обшаривают весь интернет без разбора.

Когда возникает необходимость обеспечить информационную безопасность компании, руководство, как правило, обращается к системным интеграторам. Они проводят комплексный анализ и разрабатывают проект по защите информации. В конечном счёте всё это оборачивается приобретением дорогостоящих программных и аппаратных средств, таких как Cisco PIX, Checkpoint, Microsoft ISA. Такие большие комплексные проекты стоят более 15 тыс. долл., требуют постоянного сопровождения и целесообразны только для крупных предприятий.

Для малых и многих средних предприятий весь проект по защите можно свести к двум пунктам:

1) защита персональных компьютеров;
2) комплекс из интернет-шлюза и файрвола, отгораживающий сеть предприятия от Всемирной сети и защищающий компьютеры пользователей от проникновения извне.

Рост автоматизации производственно-хозяйственных процессов крупных промышленных предприятий и активное внедрение информационных технологий привели к значительному увеличению информационной среды предприятий. Одно из следствий этого процесса - повышение вероятности утечки, потери или порчи информации, которая влияет на обеспечение безопасности объекта

Система обеспечения информационной безопасности представляет собой комплекс организационных, административно-правовых, программно-технических и иных мероприятий, направленных на защиту информационной среды. К объектам комплексной интегрированной системы обеспечения информационной безопасности (КИСОИБ) предприятия относятся:

1) информационные системы (системы, предназначенные для хранения, поиска и выдачи информации по запросам пользователей);
2) информационные процессы (процессы восприятия, накопления, обработки и передачи информации, обеспечиваемые информационными системами и средствами передачи данных);
3) информационные ресурсы - совокупность данных, представляющих ценность для предприятия и выступающих в качестве материальных ресурсов: основные и вспомогательные массивы данных, хранимые во внешней памяти и входящие документы.

К сожалению, сложные сетевые технологии достаточно уязвимы для целенаправленных атак. Причем такие атаки могут производиться удаленно, в том числе и из-за пределов национальных границ. Все это ставит новые проблемы перед разработчиками и строителями информационной инфраструктуры. Некоторые современные формы бизнеса полностью базируются на сетевых технологиях (электронная торговля, IP-телефония,

сетевое провайдерство и т.д.) и по этой причине особенно уязвимы. Потребуется здесь и международное сотрудничество в сфере законодательства и установления барьеров для сетевых террористов. Не исключено, что придется со временем модифицировать с учетом требований безопасности некоторые протоколы и программы.

В связи с актуальностью проблемы защиты информации совершенно необходимо определить объект защиты. В «Основы инженерно-технической защиты информации». Торокина А.А. отмечается: «Так как с помощью материальных средств можно защищать только материальный объект, то объектами защиты являются материальные носители информации».

Такой подход представляется конструктивным, особенно с учетом современных представлений об информации и объектах информатизации.

В словаре Ф.А. Брокгауза-И.А. Ефрона говорится: «Информация — прошение малороссийских гетманов московскому царю или польскому королю» (цитата по Шурухнову Н.Г. «Расследование неправомерного доступа к компьютерной информации», т.к. в доступном издании словаря данное определение не найдено).

Несколько по-другому определяется информация в Федеральном Законе «Об информации, информатизации и защите информации». Принят Государственной Думой 8 июля 2006., а именно, как: «сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления».

Такое разнообразие подходов есть отражение сложности проблемы. Мы же будем исходить из того, что гарантированная защита возможна лишь в том случае, когда она реализуется, начиная с момента порождения объекта защиты. Естественно, в этом случае рассматривать защиту информации как защиту ОИ и их составляющих, являющихся носителями сведений (вычислительные машины, комплексы, сети, электронные документы и т.д.).

Безопасность представляет собой комплексное понятие, куда входят технические аспекты надежности оборудования, качество питающей сети,

уязвимость программного обеспечения и т.д. Можно отключить сеть от Интернет, установить систему RAID для обеспечения дисковой защиты, снабдить систему надежным UPS, но в случае, например, пожара возможно потерять базу данных, которую создавали несколько лет. Проектируя сеть, надо с самого начала учитывать все возможные угрозы, как объективные, так и субъективные.

Число ЭВМ, подключенных в Интернет, к концу 2018 года достигло 22 миллиардов. Число WEB-серверов в 2018 году перевалило за 1 миллиард. Сегодня трудно представить себе фирму, организацию или учреждение, где бы для обработки документов, ведения бухгалтерии, учета, обмена сообщениями, доступа к информационным и поисковым серверам и так далее не использовали машин, подключенных к сети. Огромная масса людей не может себе представить жизнь без доступа к сети Интернет, который стал еще одним средством массовой информации. Но преимущества доступа к информации через сеть все чаще омрачаются атаками вирусов, червей, троянских коней, spyware и хакеров.

Одна из проблем, связанных с критериями оценки безопасности систем, заключалась в недостаточном понимании механизмов работы в сети. При объединении компьютеров к старым проблемам безопасности добавляются новые. Да, мы имеем средства связи, но при этом локальных сетей гораздо больше, чем глобальных. Скорости передачи стали выше, появилось множество линий общего пользования. Шифровальные блоки иногда отказываются работать. Существует излучение от проводки, проходящей по всему зданию. И, наконец, появились многочисленные пользователи, имеющие доступ к системам.

Целью дипломной работы является разработка и реализация политики безопасности в локальной сети на примере предприятия.

Для достижения указанной цели необходимо выполнить ряд задач:

1) выявление возможных источников угроз объектов атаки в локальной сети вуза;

2) проектирование политики безопасности корпоративной сети;
3) разработка комплекса мероприятий по защите информации в сети;
4) анализ эффективности реализации политики безопасности в сети предприятия.

1 АНАЛИЗ ПОТЕНЦИАЛЬНЫХ УГРОЗ ОПЕРАТИВНО-ТЕХНОЛОГИЧЕСКОЙ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ СЕТИ

1.1 Основные цели сетевой безопасности

Крайне важно понять, что безопасность — это не продукт, который можно купить в магазине и быть уверенным в собственной защищенности. «Безопасность» — особая комбинация как технических, так и административных мер. Административные меры также включают в себя не только бумаги, рекомендации, инструкции, но и людей. Невозможно считать свою сеть «безопасной», если вы не доверяете людям, работающим с этой сетью.

Идеальная безопасность — недостижимый миф, который могут реализовать, в лучшем случае, только несколько профессионалов. Есть один фактор, который невозможно преодолеть на пути к идеальной безопасности — это человек.

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основных целей обычно три:

1) Целостность данных;
2) Конфиденциальность данных;
3) Доступность данных.

Рассмотрим более подробно каждую из них.

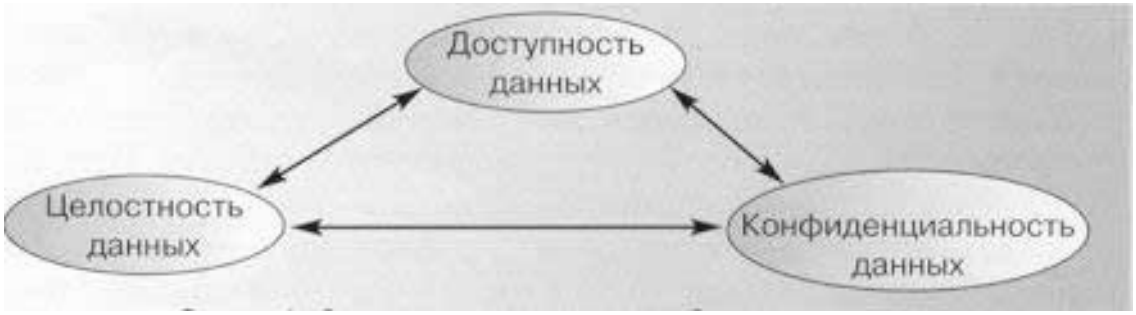

Рисунок 1. Цели сетевой безопасности

Целостность данных

Одна из основных целей сетевой безопасности — гарантированность того, чтобы данные не были изменены, подменены или уничтожены. Целостность данных должна гарантировать их сохранность как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.

Конфиденциальность данных

Второй главной целью сетевой безопасности является обеспечение конфиденциальности данных. Не все данные можно относить к конфиденциальной информации. Существует достаточно большое количество информации, которая должна быть доступна всем. Но даже в этом случае обеспечение целостности данных, особенно открытых, является основной задачей. К конфиденциальной информации можно отнести следующие данные:

1) личная информация пользователей;
2) учетные записи (имена и пароли);
3) данные о кредитных картах;
4) данные о разработках и различные внутренние документы;
5) бухгалтерская информация.

Доступность данных

Третьей целью безопасности данных является их доступность. Бесполезно говорить о безопасности данных, если пользователь не может работать с ними из-за их недоступности. Вот приблизительный список ресурсов, которые обычно должны быть «доступны» в локальной сети:

1) принтеры;
2) серверы;
3) рабочие станции;
4) данные пользователей;
5) любые критические данные, необходимые для работы.

Рассмотрим угрозы и препятствия, стоящие на пути к безопасности сети. Все их можно разделить на две большие группы: технические угрозы и человеческий фактор.

Технические угрозы:

1) ошибки в программном обеспечении;
2) различные DoS- и DDoS-атаки;
3) компьютерные вирусы, черви, троянские кони;
4) анализаторы протоколов и прослушивающие программы («снифферы»);
5) технические средства съема информации.

Ошибки в программном обеспечении

Самое узкое место любой сети. Программное обеспечение серверов, рабочих станций, маршрутизаторов и т. д. написано людьми, следовательно, оно практически всегда содержит ошибки. Чем выше сложность подобного ПО, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляет никакой опасности, некоторые же могут привести к трагическим последствиям, таким, как получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов (хранение ненужных данных на сервере, использование в качестве плацдарма для атаки и т.п.). Большинство таких уязвимостей устраняется с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких обновлений является необходимым условием безопасности сети.

DoS- и DDoS-атаки

Denial Of Service (отказ в обслуживании) — особый тип атак, направленный на выведение сети или сервера из работоспособного состояния. При DoS-атаках могут использоваться ошибки в программном обеспечении или легитимные операции, но в больших масштабах (например, посылка огромного количества электронной почты). Новый тип атак DDoS (Distributed Denial Of Service) отличается от предыдущего наличием огромного количества

компьютеров, расположенных в большой географической зоне. Такие атаки просто перегружают канал трафиком и мешают прохождению, а зачастую и полностью блокируют передачу по нему полезной информации. Особенно актуально это для компаний, занимающихся каким-либо online-бизнесом, например, торговлей через Internet.

Компьютерные вирусы, троянские кони

Вирусы — старая категория опасностей, которая в последнее время в чистом виде практически не встречается. В связи с активным применением сетевых технологий для передачи данных вирусы все более тесно интегрируются с троянскими компонентами и сетевыми червями. В настоящее время компьютерный вирус использует для своего распространения либо электронную почту, либо уязвимости в ПО. А часто и то, и другое. Теперь на первое место вместо деструктивных функций вышли функции удаленного управления, похищения информации и использования зараженной системы в качестве плацдарма для дальнейшего распространения. Все чаще зараженная машина становится активным участником DDoS-атак. Методов борьбы достаточно много, одним из них является все та же своевременная установка обновлений.

Анализаторы протоколов и «снифферы»

В эту группу входят средства перехвата передаваемых по сети данных. Такие средства могут быть как аппаратными, так и программными. Обычно данные передаются по сети в открытом виде, что позволяет злоумышленнику внутри локальной сети перехватить их. Некоторые протоколы работы с сетью (POPS, FTP) не используют шифрование паролей, что позволяет злоумышленнику перехватить их и использовать самому. При передаче данных по глобальным сетям эта проблема встает наиболее остро. По возможности следует ограничить доступ к сети неавторизированным пользователям и случайным людям.

Технические средства съема информации

Сюда можно отнести такие средства, как клавиатурные жучки, различные мини-камеры, звукозаписывающие устройства и т.д. Данная группа используется в повседневной жизни намного реже вышеперечисленных, так как, кроме наличия спецтехники, требует доступа к сети и ее составляющим.

Человеческий факторы:

1) уволенные или недовольные сотрудники;
2) промышленный шпионаж;
3) халатность;
4) низкая квалификация.

Уволенные и недовольные сотрудники

Данная группа людей наиболее опасна, так как многие из работающих сотрудников могут иметь разрешенный доступ к конфиденциальной информации. Особенную группу составляют системные администраторы, зачастую недовольные своим материальным положением или несогласные с увольнением, они оставляют «черные ходы» для последующей возможности злонамеренного использования ресурсов, похищения конфиденциальной информации и т. д.

Промышленный шпионаж

Это самая сложная категория. Если ваши данные интересны кому-либо, то этот кто-то найдет способы достать их. Взлом хорошо защищенной сети — не самый простой вариант. Очень может статься, что уборщица «тетя Глаша», моющая под столом и ругающаяся на непонятный ящик с проводами, может оказаться хакером весьма высокого класса.

Халатность

Самая обширная категория злоупотреблений: начиная с не установленных вовремя обновлений, неизмененных настроек «по умолчанию» и заканчивая несанкционированными модемами для выхода в Internet, — в результате чего злоумышленники получают открытый доступ в хорошо защищенную сеть.

Низкая квалификация

Часто низкая квалификация не позволяет пользователю понять, с чем он имеет дело; из-за этого даже хорошие программы защиты становятся настоящей морокой системного администратора, и он вынужден надеяться только на защиту периметра. Большинство пользователей не понимают реальной угрозы от запуска исполняемых файлов и скриптов и считают, что исполняемые файлы -только файлы с расширением «exe». Низкая квалификация не позволяет также определить, какая информация является действительно конфиденциальной, а какую можно разглашать. В крупных компаниях часто можно позвонить пользователю и, представившись администратором, узнать у него учетные данные для входа в сеть. Выход только один -обучение пользователей, создание соответствующих документов и повышение квалификации.

1.2 Модели безопасности

Рассмотрим некоторые известные модели безопасности.

Модель дискреционного доступа

В рамках модели контролируется доступ субъектов к объектам. Для каждой пары субъект-объект устанавливаются операции доступа (READ, WRITE и другие).

Контроль доступа осуществляется посредством механизма, который предусматривает возможность санкционированного изменения правил разграничения доступа. Право изменять правила предоставляется выделенным субъектам.

Модель дискретного доступа

В рамках модели рассматриваются механизмы распространения доступа субъектов к объектам.

Модель мандатного управления доступом Белла-Лападула

Формально записана в терминах теории отношений. Описывает механизм доступа к ресурсам системы, при этом для управления доступом используется матрица контроля доступа. В рамках модели рассматриваются

простейшие операции READ и WRITE доступа субъектов к объектам, на которые накладываются ограничения.

Множества субъектов и объектов упорядочены в соответствии с их уровнем полномочий и уровнем безопасности, соответственно.

Состояние системы изменяется согласно правилам трансформации состояний.

Модели распределенных систем (синхронные и асинхронные)

В рамках моделей субъекты выполняются на нескольких устройствах обработки. Рассматриваются операции доступа субъектов к объектам READ и WRITE, которые могут быть удаленными, что может вызвать противоречия в модели Белла-Лападула.

В рамках асинхронной модели в один момент времени несколько субъектов могут получить доступ к нескольким объектам.

Переход системы из одного состояния в другое состояние в один момент времени может осуществляться под воздействием более, чем одного субъекта.

Модель безопасности военной системы передачи данных (MMS -модель)

Формально записана в терминах теории множеств. Субъекты могут выполнять специализированные операции над объектами сложной структуры. В модели присутствует администратор безопасности для управления доступом к данным и устройствам глобальной сети передачи данных. При этом для управления доступом используются матрицы контроля доступа. В рамках модели используются операции READ, WRITE, CREATE, DELETE доступа субъектов к объектам, операции над объектами специфической структуры, а также могут появляться операции, направленные на специфическую обработку информации.

Состояние системы изменяется с помощью функции трансформации.

Модель трансформации прав доступа

Формально записана в терминах теории множеств. В рамках модели субъекту в данный момент времени предоставляется только одно право доступа. Для управления доступом применяются функции трансформации прав доступа.

Механизм изменения состояния системы основывается на применении функций трансформации состояний.

Схематическая модель

Формально записана в терминах теории множеств и теории предикатов. Для управления доступа используется матрица доступа со строгой типизацией ресурсов. Для изменения прав доступа применяется аппарат копирования меток доступа.

Иерархическая модель

Формально записана в терминах теории предикатов. Описывает управление доступом для параллельных вычислений, при этом управление доступом основывается на вычислении предикатов.

Модель безопасных спецификаций

Формально описана в аксиоматике Хоара.

Модель информационных потоков

Формально записана в терминах теории множеств. В модели присутствуют объекты и атрибуты, что позволяет определить информационные потоки. Управление доступом осуществляется на основе атрибутов объекта. Изменением состояния является изменение соотношения между объектами и атрибутами.

Вероятностные модели

В модели присутствуют субъекты, объекты и их вероятностные характеристики. В рамках модели рассматриваются операции доступа субъектов к объектам READ и WRITE. Операции доступа также имеют вероятностные характеристики.

Модель элементарной защиты

Предмет защиты помещен в замкнутую и однородную защищенную оболочку, называемую преградой. Информация со временем начинает устаревать, т.е. цена ее уменьшается. За условие достаточности защиты принимается превышение затрат времени на преодоление преграды нарушителем над временем жизни информации. Вводятся вероятность не преодоления преграды нарушителем $P_{СЗИ}$, вероятность обхода преграды нарушителем $P_{обх}$, и вероятность преодоления преграды нарушителем за время, меньшее времени жизни информации $P_{нр}$. Для введенной модели нарушителя показано, что $P_{СЗИ}= min[(1 - P_{нр})(1-P_{обх})]$, что является иллюстрацией принципа слабейшего звена. Развитие модели учитывает вероятность отказа системы и вероятность обнаружения и блокировки действий нарушителя.

Модель системы безопасности с полным перекрытием

Отмечается, что система безопасности должна иметь по крайней мере одно средство для обеспечения безопасности на каждом возможном пути проникновения в систему. Модель описана в терминах теории графов. Степень обеспечения безопасности системы можно измерить, используя лингвистические переменные. В базовой системе рассматривается набор защищаемых объектов, набор угроз, набор средств безопасности, набор уязвимых мест, набор барьеров.

Модель гарантированно защищенной системы обработки информации

В рамках модели функционирование системы описывается последовательностью доступов субъектов к объектам. Множество субъектов является подмножеством множества объектов. Из множества объектов выделено множество общих ресурсов системы, доступы к которым не могут привести к утечке информации. Все остальные объекты системы являются порожденными пользователями, каждый пользователь принадлежит множеству порожденных им объектов. При условиях, что в системе существует механизм, который для каждого объекта устанавливает породившего его пользователя; что субъекты имеют доступ только к общим ресурсам

системы и к объектам, порожденным ими, и при отсутствии обходных путей политики безопасности модель гарантирует невозможность утечки информации и выполнение политики безопасности.

Субъектно-объектная модель

В рамках модели все вопросы безопасности описываются доступами субъектов к объектам. Выделены множество объектов и множество субъектов. Субъекты порождаются только активными компонентами (субъектами) из объектов. С каждым субъектом связан (ассоциирован) некоторый объект (объекты), т.е. состояние объекта влияет на состояние субъекта. В модели присутствует специализированный субъект-монитор безопасности субъектов (МБС), который контролирует порождение субъектов.

Из упомянутых моделей для нас наибольший интерес представляет дискреционные и мандатные механизмы разграничения доступа (как наиболее распространенные), модель гарантированно защищенной системы (в силу гарантированности) и субъектно-объектная модель (рассматривающая не только доступы, но и среду, в которой они совершаются).

Под сущностью понимается любая составляющая компьютерной системы.

Субъект определяется как активная сущность, которая может инициировать запросы ресурсов и использовать их для выполнения каких-либо вычислительных заданий.

Объект определяется как пассивная сущность, используемая для хранения и получения информации.

Доступ - взаимодействие между объектом и субъектом, в результате которого происходит перенос информации между ними. Взаимодействие происходит при исполнении субъектами операций. Существуют две фундаментальные операции: операция чтения (перенос информации от объекта к субъекту) и операция записи (перенос информации от субъекта к объекту).

Данные операции являются минимально необходимым базисом для описания моделей, описывающих защищенные системы.

1.3 Виды угроз и методы защиты

Каждый ИТ-сервис или объект в совокупной инфраструктуре компании имеет определенный коэффициент риска, поэтому разработку концепции безопасности вашей корпорации следует начинать именно с всестороннего их анализа.

Другим немаловажным фактором при планировании концепции безопасности следует считать различные типы угроз каждому ключевому сервису ИТ-инфраструктуры. Эти аспекты напрямую соотносятся с факторами оценки объектов и позволяют получить информацию для последующих действий по мерам защиты. Важное правило эффективности мер — защита не должна быть избыточной!

Результаты всестороннего анализа типов угроз и оценки каждого объекта сетевой ИТ-инфраструктуры являются основой для разработки и внедрения политики безопасности. Она будет включать в себя политику управления конфигурациями и обновлениями, мониторинг и аудит систем, а также другие превентивные меры операционных политик и процедур. Обязательным условием является наличие тестовой лаборатории с уменьшенным аналогом типичной ИТ-среды корпорации. Накопленные знания и опыт, полученные при анализе угроз и уязвимостей систем, являются, по сути, уникальной базой знаний и будут служить фундаментом в построении надежной и защищенной инфраструктуры и последующем обучении персонала. Однако следует учесть, что при изменении (модернизации) инфраструктуры, добавлении новых объектов необходимо произвести повторную оценку и анализ и впоследствии модифицировать политику безопасности.

Идентификация угроз

Повышение привилегий — Получение системных привилегий через атаку с переполнением буфера, незаконное получение административных прав.

Фальсификация — Модификация данных, передаваемых по сети, модификация файлов.

Имитация — Подделка электронных сообщений, подделка ответных пакетов при аутентификации.

Раскрытие информации — Несанкционированный доступ или незаконная публикация конфиденциальной информации.

Отречение — Удаление критичного файла или совершение покупки с последующим отказом признавать свои действия.

Отказ в обслуживании — Загрузка сетевого ресурса большим количеством поддельных пакетов.

Защита на всех уровнях

Чтобы уменьшить возможность успешного вторжения в ИТ-среду корпорации, надо создать комплексные меры защиты на всех возможных уровнях. Такая концепция информационной безопасности подразумевает, что нарушение одного уровня защиты не скомпрометирует всю систему в целом.

Проектирование и построение каждого уровня безопасности должны предполагать, что любой уровень может быть нарушен злоумышленником. Кроме того, каждый из уровней имеет свои специфические и наиболее эффективные методы защиты. Из перечня доступных и разработанных многими известными вендорами технологий можно выбрать наиболее подходящую по техническим и экономическим факторам. Например:

1) защита данных — списки контроля доступа, шифрование;
2) приложения — защищенные приложения, антивирусные системы;
3) компьютеры — защита операционной системы, управление обновлениями, аутентификация, система обнаружения вторжений на уровне хоста;
4) внутренняя сеть — сегментация сети, IP Security, сетевые системы обнаружения вторжений;

5) периметр — программные и программно-аппаратные межсетевые экраны, создание виртуальных частных сетей с функциями карантина;
6) физическая защита — охрана, средства наблюдения и разграничения доступа;
7) политики и процедуры — обучение пользователей и технического персонала.

Таким образом, в результате комплексных мер защиты на всех уровнях упрощается процесс обнаружения вторжения и снижаются шансы атакующего на успех.

Человеческий фактор

Многие уровни защиты имеют в своей основе программно-аппаратные средства, однако влияние “человеческого фактора” вносит в общую картину серьезные коррективы.

Уровень физической защиты

Требования физической защиты являются базовыми и первоочередными для внедрения.

Имея физический доступ к оборудованию, злоумышленник может легко обойти последующие уровни защиты. Для доступа могут использоваться телефоны компании или карманные устройства. Особо уязвимыми с точки зрения утечки важной информации являются портативные компьютеры, которые могут находиться за пределами корпорации.



Рисунок 2. Защита корпоративной информации на

В некоторых случаях фактор доступа нацелен на нанесение вреда. Однако при наличии физического доступа можно устанавливать программные средства контроля и мониторинга за особо важной корпоративной информацией, которые будут накапливать ее в течение длительного времени.

Для обеспечения безопасности уровня физической защиты можно использовать любые доступные средства, которые позволит бюджет компании. Элементы защиты должны охватывать все компоненты ИТ-инфраструктуры. Например, инженер сервисной службы заменил вышедший из строя дисковый массив уровня RAID 10, содержавший важные данные пользователей корпорации. После этого диск может быть отправлен в сервисный центр, где его можно восстановить и получить доступ к данным. В таком случае уровень физической защиты корпорации можно считать скомпрометированным.

Первым шагом в обеспечении надежного уровня защиты является физическое разнесение серверной и пользовательской инфраструктуры. Обязательным при этом становится наличие отдельного, надежно закрытого помещения, с процедурами жесткого контроля доступа и мониторинга. Наличие персонифицированного доступа на основе магнитных карт или биометрических устройств резко уменьшает шансы злоумышленника. Серверная комната должна быть оснащена автоматическими системами пожаротушения и климат-контроля. Доступ можно дополнительно контролировать с помощью системы видеонаблюдения с возможностью записи событий.

Удаленный доступ к консолям серверов также подлежит тщательному контролю. Имеет смысл выделять административную группу в отдельный физический сегмент сети с постоянным мониторингом доступа и на сетевом уровне управляемых коммутаторов и хостов, и на логическом уровне персональной идентификации.

Последующие меры по обеспечению полного спектра физической защиты должны быть направлены на удаление и изъятие устройств ввода (приводов флоппи- и компакт-дисков) из тех компьютеров, где в них нет необходимости. Если это невозможно, обязательно следует использовать программные средства блокировки доступа к съемным носителям. В конечном итоге следует обеспечить гарантию физической защиты активного сетевого оборудования (коммутаторы, маршрутизаторы) в специальных шкафах с контролем доступа. Кроме этого, необходимо обеспечить коммутацию только тех устройств и розеток, которые действительно необходимы.

Периметр информационной системы является той частью сетевой инфраструктуры, которая наиболее открыта для атак извне. В периметр входят подключения к:

1) интернету;
2) филиалам;
3) сетям партнеров;
4) мобильным пользователям;
5) беспроводным сетям;
6) интернет-приложениям.

Важно рассматривать безопасность данного уровня в целом, а не только для конкретного направления. Возможные направления атак через периметр:

1) на сеть организации;
2) на мобильных пользователей;
3) со стороны партнеров;
4) со стороны филиалов;
5) на сервисы интернета;
6) из интернета.

Традиционно считается, что наиболее уязвимым является направление из интернета, однако угроза из других направлений не менее существенна. Важно, чтобы все входы и выходы в (из) вашей сети были надежно защищены. Нельзя быть уверенным в отношении мер защиты в сетевых инфраструктурах

бизнес-партнеров или филиалов, поэтому данному направлению также следует уделить пристальное внимание.

Обеспечение безопасности периметра достигается, прежде всего, использованием межсетевых экранов. Их конфигурация, как правило, технически достаточно сложна и требует высокой квалификации обслуживающего персонала, а также тщательного документирования настроек. Современные операционные системы позволяют легко блокировать неиспользуемые порты, чтобы уменьшить вероятность атаки.

Трансляция сетевых адресов (NAT) позволяет организации замаскировать внутренние порты. При передаче информации через незащищенные каналы надо использовать методы построения виртуальных частных сетей (VPN) на основе шифрования и туннелирования.

Угрозы и защита локальной сети

Атаки могут производиться не только из внешних источников. По статистике, очень большой процент удачных атак принадлежит вторжениям изнутри сетевой среды. Очень важно построить внутреннюю сетевую безопасность, чтобы остановить злонамеренные и случайные угрозы. Неконтролируемый доступ к внутренней сетевой инфраструктуре позволяет атакующему получить возможность доступа к важным данным корпорации, контролировать сетевой трафик. Полностью маршрутизируемые сети позволяют злоумышленнику получить доступ к любому ресурсу из любого сегмента сети. Сетевые операционные системы имеют множество установленных сетевых сервисов, каждый из которых может стать объектом атаки.

Для защиты внутреннего сетевого окружения надо обеспечить механизмы надежной аутентификации пользователей в глобальной службе каталогов (едином центре входа). Взаимная аутентификация на уровне сервера и сетевой рабочей станции значительно поднимает качество сетевой безопасности. Современные требования подразумевают наличие управляемой коммутируемой сетевой среды и разделение на логические сегменты (VLAN). Для администрирования удаленных устройств надо всегда использовать подключение по защищенному протоколу (например SSH). Трафик Telnet-подключений может быть легко перехвачен, а имена и пароли передаются в открытом виде. Максимум внимания — защите резервных копий конфигураций сетевых устройств, — они могут многое рассказать о топологии сети злоумышленнику.

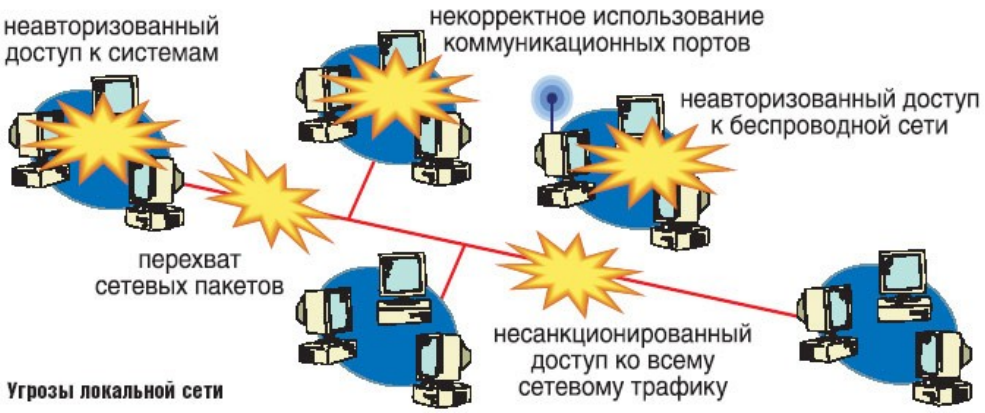

Рисунок 3. Угрозы локальной сети

Защищать сетевой трафик следует даже после проведения сегментации сети. И для проводных, и для беспроводных подключений можно использовать протокол 802.1X, чтобы обеспечить зашифрованный и аутентифицированный доступ. Это решение может использовать учетные записи и пароли в глобальной службе каталогов (Microsoft Active Directory, Novell e-Directory и т. п.) либо цифровые сертификаты. Технология цифровых сертификатов обеспечивает очень высокий уровень защиты сетевого

транспорта, однако требует развертывания инфраструктуры публичных ключей (Public Key Infrastructure) в виде сервера и хранилища сертификатов.

Внедрение технологий шифрования и цифровых подписей типа IPSec или Server Message Block (SMB) Signing воспрепятствует перехвату сетевого трафика и его анализу.

Компьютерные системы в сетевой среде выполняют некоторые задачи, которые и определяют требования защиты. Сетевые хосты могут подвергаться нападению, поскольку они является публично доступными. Злоумышленники могут распространять вредоносный код (вирусы) для осуществления распределенной атаки. Установленное на рабочих станциях и серверах программное обеспечение может иметь уязвимости в программном коде, поэтому своевременная установка обновлений — один из важных шагов в общей концепции защиты.

Настройки политики защиты уровня компьютера необходимо обеспечивать и контролировать централизованно, например, с помощью групповой политики (Group Policy). Защита серверных систем на этом уровне будет включать в себя установку атрибутов безопасности для файловых систем, политики аудита, фильтрации портов и других мер в зависимости от роли и назначения сервера.

Наличие всех доступных обновлений для операционной системы и программного обеспечения кардинально улучшает общий уровень обеспечения безопасности. Можно использовать любые способы автоматической установки и контроля обновлений, от самых простых — Windows Update, Software Update Service (SUS), Windows Update Service (WUS) до наиболее сложных и мощных — Systems Management Server (SMS).

Использование антивирусного пакета с актуальными обновлениями, персональных брандмауэров с фильтрацией портов позволит резко сократить шансы на атаку.

Защита компьютеров:

1) взаимная аутентификация пользователей, серверов и рабочих станций;
2) защита операционной системы;
3) установка обновлений безопасности;
4) аудит успешных и неуспешных событий;
5) отключение неиспользуемых сервисов;
6) установка и обновление антивирусных систем;
7) защита приложений.

Сетевые приложения дают возможность пользователям получать доступ к данным и оперировать ими. Сетевое приложение — это точка доступа к серверу, где это приложение выполняется. В этом случае приложение обеспечивает определенный уровень сетевого сервиса, который должен быть устойчив к атакам злоумышленников. Следует провести тщательное исследование как собственных разработок, так и используемых коммерческих продуктов на наличие уязвимостей. Целью атаки может быть и разрушение кода приложения (как следствие — его недоступность), и исполнение вредоносного кода. Нападавший также может применить тактику распределенной атаки, направленной на перегрузку производительности приложения. Результатом может стать отказ в облуживании (Denial of Service).

Приложение также может быть использовано в непредусмотренных задачах, например маршрутизация почтовых сообщений (открытый почтовый релей). Приложения должны быть установлены и настроены только с необходимым уровнем функциональности и сервиса, а работу программного кода можно контролировать системами мониторинга и антивирусными пакетами. Чтобы уменьшить уровень угроз, выполнение приложения следует ограничить минимальными сетевыми привилегиями.

Копрометация и защита приложений:

1) использование только необходимых служб и функций приложений;
2) настройка параметров защиты приложений;
3) установка обновлений безопасности;

4) запуск приложений в контексте с минимальными привилегиями;

5) установка и обновление антивирусных систем;

6) защита данных.

Финальный уровень — это защита данных, которые могут располагаться и на серверных хостах, и на локальных. На этом уровне следует защитить информацию, используя современные файловые системы с контролем атрибутов доступа на уровне томов, папок и файлов. Расширенные функции файловой системы, такие как аудит и шифрование, позволят более надежно построить систему разграничения доступа и осуществить надежную сохранность данных. Злоумышленник, получивший доступ к файловой системе, может причинить огромный ущерб в виде хищения, информации. Особое уделить файловым сетевой опорной глобальным службам или удаление этой печальные последствия.

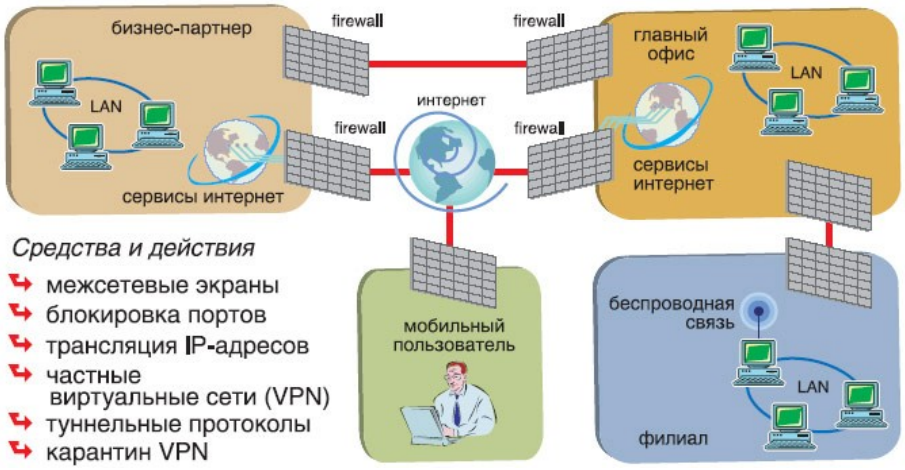

Рисунок 4. Защита информационного периметра

Например, служба каталогов Active Directory использует для хранения своей информации файлы. По умолчанию эти файлы располагаются в известном каталоге, имя которого указывается по умолчанию при генерации контроллера домена. Изменив месторасположение данных файлов путем перенесения на другой том, можно возвести огромный барьер для атакующего.

Шифрованная файловая система является еще одним важным элементом надежного бастиона защиты. Однако следует помнить, что файлы только хранятся в зашифрованном виде, а передаются через сеть открыто. Кроме того, шифрование защищает от неправомерного чтения, а защиты от удаления оно не дает. Чтобы предотвратить несанкционированное удаление, следует использовать атрибуты доступа.

Поскольку данные являются основой современного бизнеса, очень важно предусмотреть процедуры резервного копирования и восстановления. Важно также обеспечить регулярность проведения этих действий. Но следует учесть, что резервные копии являются ценным источником и лакомым куском для хищения, поэтому их сохранности нужно уделить внимание на уровне безопасности серверной комнаты.

После переноса файлов на другой, например сменный, носитель атрибуты доступа теряются. Есть, правда, технология контроля доступа к цифровым документам Windows Rights Management Services (RMS), которая обеспечивает уровень защиты независимо от месторасположения документа. RMS обладает расширенными возможностями, такими как, например, возможность просмотра документа, но запрет печати или копирования содержимого, запрет пересылки содержимого письма другому адресату, если речь идет о почтовых сообщениях.

Защита данных

Защита файлов средствами шифрующей файловой системы (EFS) Настройка ограничений в списках контроля доступа Система резервного копирования и восстановления

Защита на уровне документов с помощью Windows Right Management Services.

2 ПРОЕКТИРОВАНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЛОКАЛЬНОЙ СЕТИ

2.1 Понятие политики безопасности. Межсетевой экран как инструмент реализации политики безопасности

В столь важной задаче, как обеспечение безопасности информационной системы, нет и не может быть полностью готового решения. Это связано с тем, что структура каждой организации, функциональные связи между ее подразделениями и отдельными сотрудниками практически никогда полностью не повторяются. Только руководство организации может определить, насколько критично нарушение безопасности для компонент информационной системы, кто, когда и для решения каких задачах может использовать те или иные информационные сервисы. Ключевым этапом для построения надежной информационной системы является выработка политики безопасности.

Под политикой безопасности мы будем понимать совокупность документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов.

С практической точки зрения политику безопасности целесообразно разделить на три уровня:

Решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации.

Вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных систем, эксплуатируемых организацией.

Конкретные сервисы информационной системы.

Третий уровень включает в себя два аспекта - цели (политики безопасности) и правила их достижения, поэтому его порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, третий должен быть гораздо детальнее. У отдельных сервисов есть много свойств, которые нельзя единым образом регламентировать в рамках всей организации. В то же

время эти свойства настолько важны для обеспечения режима безопасности, что решения, относящиеся к ним, должны приниматься на управленческом, а не техническом уровне.

В рассматриваемом случае существенна политика безопасности, формируемая на двух нижних уровнях. Для того, чтобы рассмотреть ее более конкретно, необходимо определить сущность и основные функциональные свойства межсетевого экрана - инструмента проведения этой политики.

Рассмотрим структуру информационной системы предприятия (организации). В общем случае она представляет собой неоднородный набор (комплекс) из различных компьютеров, управляемых различными операционными системами и сетевого оборудования, осуществляющего взаимодействие между компьютерами. Поскольку описанная система весьма разнородна (даже компьютеры одного типа и с одной ОС могут, в соответствии с их назначением, иметь совершенно различные конфигурации), вряд ли имеет смысл осуществлять защиту каждого элемента в отдельности. В связи с этим предлагается рассматривать вопросы обеспечения информационной безопасности для локальной сети в целом. Это оказывается возможным при использовании межсетевого экрана (firewall).

Концепция межсетевого экранирования формулируется следующим образом.

Пусть имеется два множества информационных систем. Экран — это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран выполняет свои функции, контролируя все информационные потоки между двумя множествами систем (рисунок 5).

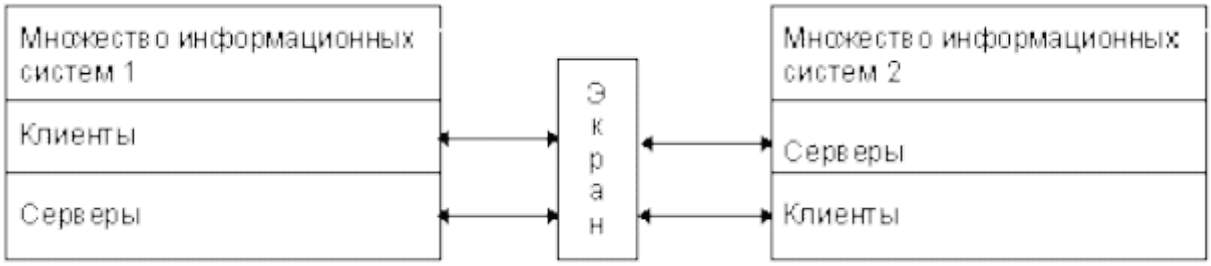

Рисунок 5. Экран как средство разграничения доступа

В простейшем случае экран состоит из двух механизмов, один из которых ограничивает перемещение данных, а второй, наоборот, ему способствует (то есть осуществляет перемещение данных). В более общем случае экран (полупроницаемую оболочку) удобно представлять себе как последовательность фильтров. Каждый из них может задержать (не пропустить) данные, а может и сразу "перебросить" их "на другую сторону". Кроме того, допускается передача порции данных на следующий фильтр для продолжения анализа, или обработка данных от имени адресата и возврат результата отправителю (рисунок 6).

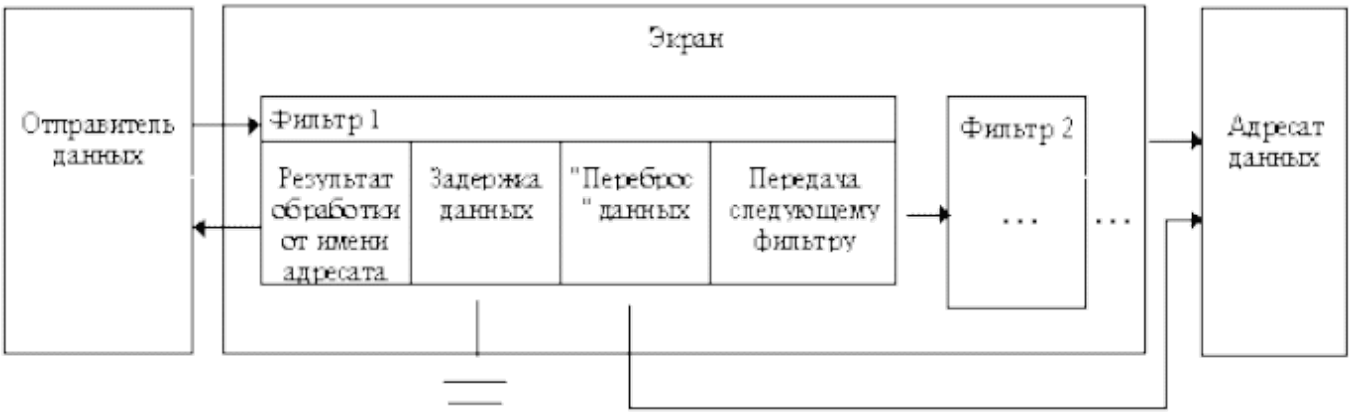

Рисунок 6. Экран как последовательность фильтров

Помимо функций разграничения доступа, экраны осуществляют также протоколирование информационных обменов.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней. Так, межсетевые экраны устанавливают для защиты локальной сети организации, имеющей выход в открытую среду, подобную Internet. Другой пример экрана - устройство защиты порта, контролирующее доступ к коммуникационному порту компьютера до и независимо от всех прочих системных защитных средств. Экранирование позволяет поддерживать доступность сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, индуцированную внешней активностью. Уменьшается уязвимость внутренних

сервисов безопасности, поскольку первоначально сторонний злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно и жестко. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности. Чаще всего экран реализуют как сетевой сервис на третьем (сетевом), четвертом (транспортном) или седьмом (прикладном) уровнях семиуровневой эталонной модели OSI. В первом случае мы имеем экранирующий маршрутизатор, во втором - экранирующий транспорт, в третьем - экранирующий шлюз. Каждый подход имеют свои достоинства и недостатки; известны также гибридные экраны, где делается попытка объединить лучшие качества упомянутых подходов.

Экранирующий маршрутизатор имеет дело с отдельными пакетами данных, поэтому иногда его называют пакетным фильтром. Решения о том, пропустить или задержать данные, принимаются для каждого пакета независимо, на основании анализа полей заголовков сетевого и (быть может) транспортного уровней, путем применения заранее заданной системы правил. Еще один важный компонент анализируемой информации - порт, через который пакет поступил в маршрутизатор.

Современные маршрутизаторы (такие, как продукты компаний Bay Networks или Cisco) позволяют связывать с каждым портом несколько десятков правил и фильтровать пакеты как на входе (при поступлении в маршрутизатор), так и на выходе. В принципе, в качестве пакетного фильтра может использоваться и универсальный компьютер, снабженный несколькими сетевыми картами. Основные достоинства экранирующих маршрутизаторов - дешевизна (на границе сетей маршрутизатор нужен практически всегда, дело лишь в том, чтобы задействовать его экранирующие возможности) и

прозрачность для более высоких уровней модели OSI. Основной недостаток - ограниченность анализируемой информации и, как следствие. относительная слабость обеспечиваемой защиты.

Экранирующий транспорт позволяет контролировать процесс установления виртуальных соединений и передачу информации по ним. С точки зрения реализации экранирующий транспорт представляет собой довольно простую, а значит, надежную программу. Пример экранирующего транспорта - продукт TCP wrapper.

По сравнению с пакетными фильтрами, экранирующий транспорт обладает большей информацией, поэтому он может осуществлять более тонкий контроль за виртуальными соединениями (например, он способен отслеживать количество передаваемой информации и разрывать соединения после превышения определенного предела, препятствуя тем самым несанкционированному экспорту информации). Аналогично, возможно накопление более содержательной регистрационной информации. Главный недостаток - сужение области применимости, поскольку вне контроля остаются датаграммные протоколы. Обычно экранирующий транспорт применяют в сочетании с другими подходами, как важный дополнительный элемент. Экранирующий шлюз, функционирующий на прикладном уровне, способен обеспечить наиболее надежную защиту. Как правило, экранирующий шлюз представляет собой универсальный компьютер, на котором функционируют программные агенты - по одному для каждого обслуживаемого прикладного протокола. При подобном подходе, помимо фильтрации, реализуется еще один важнейший аспект экранирования. Субъекты из внешней сети видят только шлюзовой компьютер; соответственно, им доступна только та информация о внутренней сети, которую шлюз считает нужным экспортировать. Шлюз на самом деле экранирует, то есть заслоняет, внутреннюю сеть от внешнего мира. В то же время субъектам внутренней сети кажется, что они напрямую общаются с объектами внешнего мира. Недостаток экранирующих шлюзов - отсутствие

полной прозрачности, требующее специальных действий для поддержки каждого прикладного протокола.

Примером инструментария для построения экранирующих шлюзов является TIS Firewall Toolkit компании Trusted Information Systems.

В гибридных системах, таких как Firewall-1 компании Sun Microsystems, действительно удается объединить лучшие качества экранирующих систем, то есть получить надежную защиту, сохранить прозрачность для приложений и удержать накладные расходы в разумных пределах. Кроме того, появляются и очень ценные новые возможности, такие как отслеживание передачи информации в рамках датаграммных протоколов.

Важным понятием экранирования является зона риска, которая определяется как множество систем, которые становятся доступными злоумышленнику после преодоления экрана или какого-либо из его компонентов. Как правило, для повышения надежности защиты экран реализуют как совокупность элементов, так что "взлом" одного из них еще не открывает доступ ко всей внутренней сети. Пример возможной конфигурации многокомпонентного экрана представлен на рисунке 7.

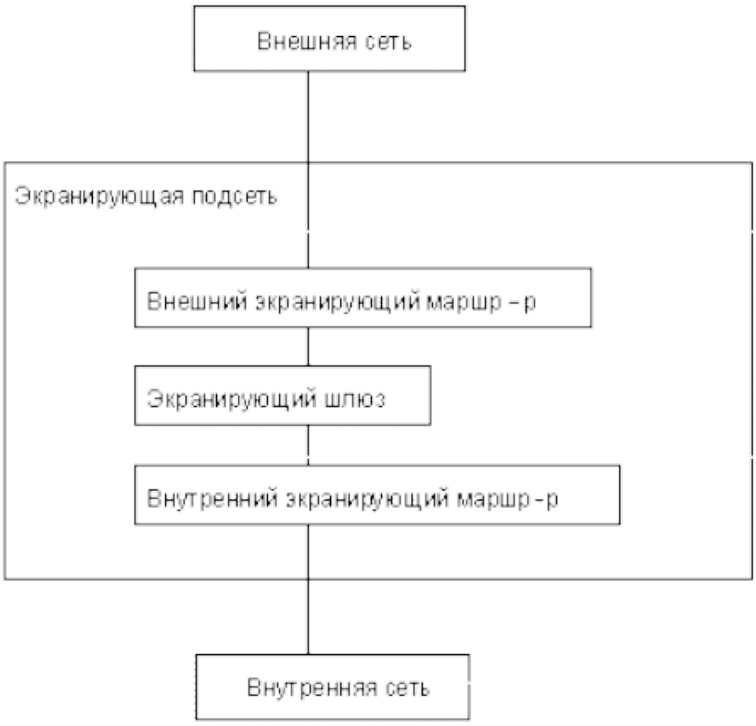

Рисунок 7. Многокомпонентный экран

Рассмотрим требования к реальной системе, осуществляющей межсетевое экранирование. В большинстве случаев экранирующая система должна:

Обеспечивать безопасность внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи;

Обладать мощными и гибкими средствами управления для полного и, насколько возможно, простого воплощения в жизнь политики безопасности организации. Кроме того, экранирующая система должна обеспечивать простую реконфигурацию системы при изменении структуры сети;

Работать незаметно для пользователей локальной сети и не затруднять выполнение ими легальных действий;

Работать достаточно эффективно и успевать обрабатывать весь входящий и исходящий трафик в "пиковых" режимах. Это необходимо для того, чтобы firewall нельзя было, образно говоря, "забросать" большим количеством вызовов, которые привели бы к нарушению работы;

Обладать свойствами самозащиты от любых несанкционированных воздействий, поскольку межсетевой экран является ключом к конфиденциальной информации в организации;

Если у организации имеется несколько внешних подключений, в том числе и в удаленных филиалах, система управления экранами должна иметь возможность централизованно обеспечивать для них проведение единой политики безопасности;

Иметь средства авторизации доступа пользователей через внешние подключения. Типичной является ситуация, когда часть персонала организации должна выезжать, например, в командировки, и в процессе работы им требуется доступ, по крайней мере, к некоторым ресурсам внутренней компьютерной сети организации. Система должна надежно распознавать таких пользователей и предоставлять им необходимые виды доступа.

Экранирование позволяет поддерживать доступность сервисов внутри информационной системы, уменьшая или вообще ликвидируя нагрузку, инициированную внешней активностью. Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно и жестко. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более надежным образом. Экранирование дает возможность контролировать информационные потоки, направленные во внешнюю область, обеспечивая режим конфиденциальности.

Таким образом, экранирование в сочетании с другими мерами безопасности использует идею многоуровневой защиты. За счет этого внутренняя сеть подвергается риску только в случае преодоления нескольких, по-разному организованных защитных рубежей.

Наличие инструмента межсетевого экранирования позволяет использовать его и для контроля доступа к информационным ресурсам организации по коммутируемым каналам связи. Для этого необходимо использовать устройство, называемое терминальным сервером. Терминальный сервер представляет собой программно-аппаратную конфигурацию, рассмотренную в следующем разделе. В качестве средства работы с коммутируемыми каналами связи предлагается терминальный сервер "Annex" компании "Bay Networks".

2.2 Особенности и преимущества предлагаемого решения.

Разработка и коррекция правил политики безопасности

Конфигурация межсетевого экрана с экранирующей подсетью является одной из наиболее надежных на сегодняшний день. Причиной этому является наличие по крайней мере трех уровней защиты:

1) внешний экранирующий маршрутизатор;
2) экранирующий шлюз;

3) внутренний экранирующий маршрутизатор.

Слабые места каждой из этих систем различны. Экранирующая подсеть позволяет также простое включение коммутируемых каналов связи в общий контур обеспечения безопасности. Критичным в случае предлагаемого решения будет эффективность работы экранирующего шлюза, его способность эффективно перерабатывать проходящую через экран информацию. Это, в свою очередь, требует установки программного обеспечения с малыми потерями в производительности системы на экранирующий компьютер-шлюз, который сам достаточно надежно защищен встроенными средствами ОС - например, компьютер фирмы SUN под управлением ОС Solaris с программой межсетевого экранирования Firewall-1.

Программа межсетевого экранирования Firewall-1 является лидером в своем классе программ - на ее основе построено более 4000 систем, что в четыре раза больше, чем у следующего за ним продукта. Причиной этому является ряд отличительных черт, которыми обладает указанная программа:

1) высокая надежность, обеспечивающаяся как работой на уровне фильтрации сетевых пакетов, так и на уровне приложений;

2) централизованное управление работой нескольких фильтрующих модулей;

3) возможность работы с любым сетевым сервисом, как стандартным, так и определенным пользователем;

4) возможность фильтрации UDP пакетов;

5) возможность управления фильтрами маршрутизаторов компаний Bay Networks и CISCO;

6) высокая эффективность работы: использование Firewall-1 уменьшает пропускную способность информационного канала не более, чем на 10%;

7) полная прозрачность работы сервисов и приложений для пользователей;

8) дополнительная аутентификация клиентов для большого набора сервисов;

9) дружественный интерфейс, позволяющий легко перестраивать правила фильтрации, описывая их в терминах политики безопасности;

10) для каждого правила (политики доступа) могут быть определены условия протоколирования, оповещения администратора либо иной реакции системы;

11) средства проверки правил работы фильтра на внутреннюю непротиворечивость;

12) средства мониторинга состояния компонент системы, позволяющие своевременно обнаружить попытку нападения на нее;

13) средства детального протоколирования и генерации отчетов;

14) трансляция адресов локальной сети, позволяющая реализовать как дополнительную защиту компьютеров локальной сети, так и более эффективное использование официального набора IP-адресов.

Простота установки и администрирования.

Одним из наиболее распространенных средств аутентификации удаленных пользователей является программа S/key компании Bellcore. Эта программа представляет собой средство обмена одноразовыми паролями, что делает невозможным несанкционированный доступ в систему, даже если эта информация кем-либо перехвачена. Программа S/key совместима со средствами аутентификации системы Firewall-1.

При конфигурировании межсетевых экранов основные конструктивные решения заранее задаются политикой безопасности, принятой в организации. В описываемом случае необходимо рассмотреть два аспекта политики безопасности: политику доступа к сетевым сервисам и политику межсетевого экрана.

При формировании политики доступа к сетевым сервисам должны быть сформулированы правила доступа пользователей к различным сервисам,

используемым в организации. Этот аспект, таким образом состоит из двух компонент.

База правил для пользователей описывает, когда, какой пользователь (группа пользователей) каким сервисом и на каком компьютере может воспользоваться. Отдельно определяются условия работы пользователей вне локальной сети организации, равно как и условия их аутентификации.

База правил для сервисов описывает набор сервисов, проходящих через сетевой экран, а также допустимые адреса клиентов серверов для каждого сервиса (группы сервисов).

В политике, регламентирующей работу межсетевого экрана, решения могут быть приняты как в пользу безопасности в ущерб легкости использования, так и наоборот. Есть два основных:

1) все, что не разрешено, то запрещено;
2) все, что не запрещено, то разрешено.

В первом случае межсетевой экран должен быть сконфигурирован таким образом, чтобы блокировать все, а его работа должна быть упорядочена на основе тщательного анализа опасности и риска. Это напрямую отражается на пользователях и они, вообще говоря, могут рассматривать экран просто как помеху. Такая ситуация заставляет накладывать повышенные требования на производительность экранирующих систем и повышает актуальность такого свойства, как "прозрачность" работы межсетевого экрана с точки зрения пользователей. Первый подход является более безопасным, поскольку предполагается, что администратор не знает, какие сервисы или порты безопасны, и какие "дыры" могут существовать в ядре или приложении разработчика программного обеспечения. Ввиду того, что многие производители программного обеспечения не спешат публиковать обнаруженные недостатки, существенные для информационной безопасности (что характерно для производителей так называемого "закрытого" программного обеспечения, крупнейшим из которых является Microsoft), этот

подход является, несомненно, более консервативным. В сущности, он является признанием факта, что незнание может причинить вред.

Во втором случае, системный администратор работает в режиме реагирования, предсказывая, какие действия, отрицательно воздействующие на безопасность, могут совершить пользователи либо нарушители, и готовит защиту против таких действий. Это существенно восстанавливает администратора firewall против пользователей в бесконечных "гонках вооружений", которые могут оказаться весьма изматывающими. Пользователь может нарушить безопасность информационной системы, если не будет уверен в необходимости мер, направленных на обеспечение безопасности.

2.3 Методика построения корпоративной системы защиты информации

Большинство директоров служб автоматизации (CIO) и информационной безопасности (CISO) российских компаний наверняка задавалось вопросом: “Как оценить уровень защищенности информационных активов компании и определить перспективы развития корпоративной системы защиты информации?”. Давайте попробуем найти ответ на этот актуальный вопрос.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории России. Поэтому решение вопроса об оценке уровня защищенности информационных активов компании обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации. Вследствие этого, в дополнение к требованиям и рекомендациям стандартов, Конституции и федеральным законам, руководящим документам Гостехкомиссии России и ФАПСИ, приходится использовать ряд международных рекомендаций. В том числе адаптировать к отечественным условиям и применять на практике методики международных

стандартов, таких, как ISO 17799, 9001, 15408, BSI и другие, а также использовать методики управления информационными рисками в совокупности с оценками экономической эффективности инвестиций в обеспечение защиты информации компании.

Современные методики управления рисками, проектирования и сопровождения корпоративных систем защиты информации должны позволять решить ряд задач перспективного стратегического развития компании.

Во-первых, количественно оценить текущий уровень информационной безопасности компании, что потребует выявления рисков на правовом, организационно-управленческом, технологическом, а также техническом уровнях обеспечения защиты информации.

Во-вторых, разработать и реализовать комплексный план совершенствования корпоративной системы защиты информации для достижения приемлемого уровня защищенности информационных активов компании. Для этого необходимо:

1) обосновать и произвести расчет финансовых вложений в обеспечение безопасности на основе технологий анализа рисков, соотнести расходы на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;
2) выявить и провести первоочередное блокирование наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы;
3) определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц по обеспечению информационной безопасности компании, создать необходимый пакет организационно-распорядительной документации;
4) разработать и согласовать со службами организации, надзорными органами проект внедрения необходимых комплексов защиты, учитывающий современный уровень и тенденции развития информационных технологий;

5) обеспечить поддержание внедренного комплекса защиты в соответствии с изменяющимися условиями работы организации, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты.

Работы, поддерживающие практическую реализацию плана информационной безопасности, в частности, заключаются в следующем:

1) разработка технического проекта модернизации средств защиты ИС, установленных на фирме по результатам проведенного комплексного аналитического исследования корпоративной сети;
2) подготовка компании к аттестации (к аттестации объектов информатизации заказчика на соответствие требованиям руководящих документов Гостехкомиссии при Президенте РФ, а также на соответствие требованиям безопасности международных стандартов ISO 15408, ISO 17799, стандарта ISO 9001 при обеспечении требований информационной безопасности компании);
3) разработка расширенного перечня сведений ограниченного распространения как части политики безопасности;
4) разработка пакета организационно-распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ компании на организационно-управленческом и правовом уровне;
5) поставка комплекта типовой организационно-распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ компании на организационно-управленческом и правовом уровнях.

Уровень информационной безопасности компании во многом зависит от квалификации специалистов. В целях повышения квалификации и переподготовки кадров рекомендуется проводить тренинги по применению средств защиты информации, технологии защиты информации, обучать сотрудников основам экономической безопасности.

Немаловажную роль играет и ежегодная переоценка состояния информационной безопасности компании.

В соответствии со ст. 20 Федерального закона “Об информации, информатизации и защите информации” целями защиты информации являются в том числе: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

Главная цель любой системы информационной безопасности заключается в обеспечении устойчивого функционирования объекта: предотвращении угроз его безопасности, защите законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, предусмотренных Уголовным кодексом РФ, обеспечении нормальной производственной деятельности всех подразделений объекта. Другая задача сводится к повышению качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов**.**

Для этого необходимо:

1) отнести информацию к категории ограниченного доступа (служебной тайне);
2) прогнозировать и своевременно выявлять угрозы безопасности информационным ресурсам, причины и условия, способствующие нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
3) создать условия функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;
4) создать механизм и условия оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций

в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;

5) создать условия для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, и тем самым ослабить возможное негативное влияние последствий нарушения информационной безопасности.

При выполнении работ можно использовать следующую модель построения корпоративной системы защиты информации (рисунок 8), основанную на адаптации Общих Критериев (ISO 15408) и проведении анализа риска (ISO 17799). Эта модель соответствует специальным нормативным документам по обеспечению информационной безопасности, принятым в Российской Федерации, международному стандарту ISO/IEC 15408 “Информационная технология – методы защиты – критерии оценки информационной безопасности”, стандарту ISO/IEC 17799 “Управление информационной безопасностью” и учитывает тенденции развития отечественной нормативной базы (в частности, Гостехкомиссии РФ) по вопросам защиты информации.



Рисунок 8. Модель построения корпоративной системы защиты информации

Представленная модель защиты информации – это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Рассматриваются следующие объективные факторы:

1) угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;
2) уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;
3) риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в

конечном итоге отражает вероятные финансовые потери – прямые или косвенные).

Для построения сбалансированной системы информационной безопасности предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для организации на основе заданного критерия. Систему информационной безопасности (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

Предлагаемая методика проведения аналитических работ позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности, избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, обеспечить проведение работ в сжатые сроки, представить обоснование для выбора мер противодействия, оценить эффективность контрмер, сравнить различные варианты контрмер.

В ходе работ должны быть установлены границы исследования. Для этого необходимо выделить ресурсы информационной системы, для которых в дальнейшем будут получены оценки рисков. При этом предстоит разделить рассматриваемые ресурсы и внешние элементы, с которыми осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные, а также в соответствии со ст. 2 Федерального закона “Об информации, информатизации и защите информации” – информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Примерами внешних элементов являются сети связи (абз. 4 ст. 2 Федерального закона “О связи”), внешние сервисы и т.п.

При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения ИБ.

Эта модель, в соответствии с предлагаемой методикой, строится следующим образом: для выделенных ресурсов определяется их ценность, как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т.д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут рекомендации по проведению регулярных проверок эффективности системы защиты.

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

По завершении работ, можно будет определить меру гарантии безопасности информационной среды, основанную на оценке, с которой можно доверять информационной среде объекта. Данный подход предполагает, что большая гарантия следует из применения больших усилий при проведении оценки безопасности. Адекватность оценки основана на

вовлечении в процесс оценки большего числа элементов информационной среды объекта, глубине, достигаемой за счет использования при проектировании системы обеспечения безопасности большего числа проектов и описаний деталей выполнения, строгости, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

Формирование организационной политики безопасности

Прежде чем предлагать какие-либо решения по системе информационной безопасности, предстоит разработать политику безопасности. Организационная политика безопасности описывает порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Этапы построения организационной политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности.

Организационная политика безопасности оформляется в виде отдельного документа, который согласовывается и утверждается Заказчиком.

Прежде всего, необходимо составить детализированное описание общей цели построения системы безопасности объекта, выражаемое через совокупность факторов или критериев, уточняющих цель. Совокупность факторов служит базисом для определения требований к системе (выбор альтернатив). Факторы безопасности, в свою очередь, могут распределяться на правовые, технологические, технические и организационные.

Требования гарантии достигаемой защиты выражаются через оценки функций безопасности СИБ объекта. Оценка силы функции безопасности

выполняется на уровне отдельного механизма защиты, а ее результаты позволяют определить относительную способность соответствующей функции безопасности противостоять идентифицированным угрозам. Исходя из известного потенциала нападения, сила функции защиты определяется, например, категориями “базовая”, “средняя”, “высокая”. Потенциал нападения определяется путем экспертизы возможностей, ресурсов и мотивов побуждения нападающего.

Перечень требований к системе информационной безопасности, эскизный проект, план защиты (далее – техническая документация, ТД) содержит набор требований безопасности информационной среды объекта, которые могут ссылаться на соответствующий профиль защиты, а также содержать требования, сформулированные в явном виде.

В общем виде разработка ТД включает:

1) уточнение функций защиты;
2) выбор архитектурных принципов построения СИБ;
3) разработку логической структуры СИБ (четкое описание интерфейсов);
4) уточнение требований функций обеспечения гарантоспособности СИБ;
5) разработку методики и программы испытаний на соответствие сформулированным требованиям.

На этапе оценки достигаемой защищенности производится оценка меры гарантии безопасности информационной среды. Мера гарантии основывается на оценке, с которой после выполнения рекомендованных мероприятий можно доверять информационной среде объекта. Базовые положения данной методики предполагают, что степень гарантии следует из эффективности усилий при проведении оценки безопасности. Увеличение усилий оценки предполагает:

1) значительное число элементов информационной среды объекта, участвующих в процессе оценивания;

2) расширение типов проектов и описаний деталей выполнения при проектировании системы обеспечения безопасности;
3) строгость, заключающуюся в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

В целом рассмотренная выше методика позволяет оценить или переоценить уровень текущего состояния защищенности информационных активов компании, а также выработать рекомендации по обеспечению (повышению) информационной безопасности компании. В том числе снизить потенциальные потери компании путем повышения устойчивости функционирования корпоративной сети, разработать концепцию и политику безопасности компании. Также рассмотренная методика позволяет предложить планы защиты конфиденциальной информации компании, передаваемой по открытым каналам связи, защиты информации компании от умышленного искажения (разрушения), несанкционированного доступа к ней, ее копирования или использования.

3 РЕАЛИЗАЦИЯ КОМПЛЕКСА МЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ СЕТИ

3.1 Информационная модель системы управления предприятием ООО «АйТиЭл»

ООО «АйТиЭл» было создано в апреле 2018 года. Компания занимается ремонтом, обслуживанием и продажей компьютерной техники. Юридический адрес компании: г. Калининград, ул. Дм. Донского, 11, офис 616

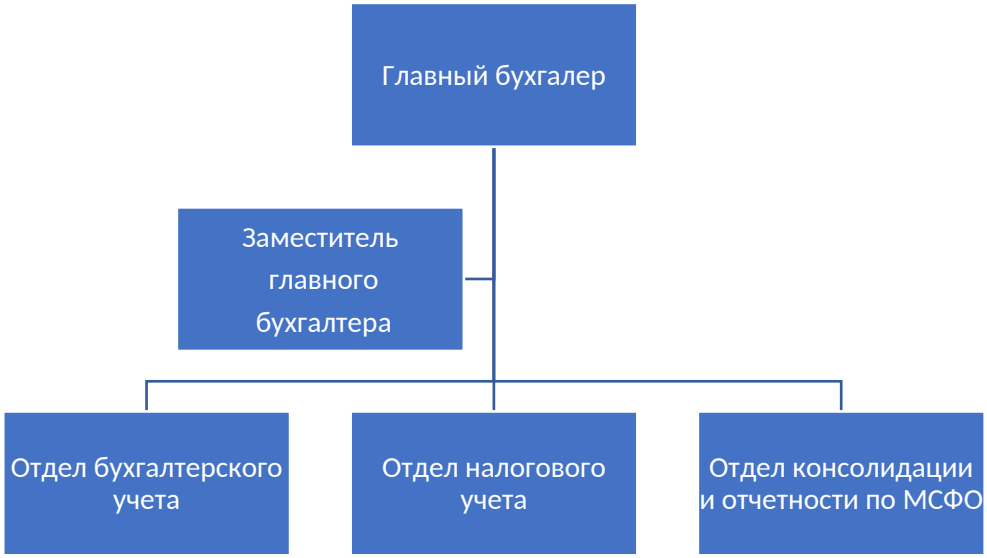

Рисунок 9. Структура подразделения бухгалтерии ООО «АйТиЭл»

Главный бухгалтер несет ответственность за формирование Учетной политики, ведение бухгалтерского учета, своевременное представление полной и достоверной бухгалтерской отчетности, обеспечивает соответствие хозяйственных операций законодательству Российской Федерации, контроль за движением имущества и выполнением обязательств.

Для построения информационной модели системы управления необходимо четко представлять структуру информационных потоков организации. Составим схематически существующую структуру информационной модели предприятия, основываясь на организационно-штатной структуре (рисунок 9).

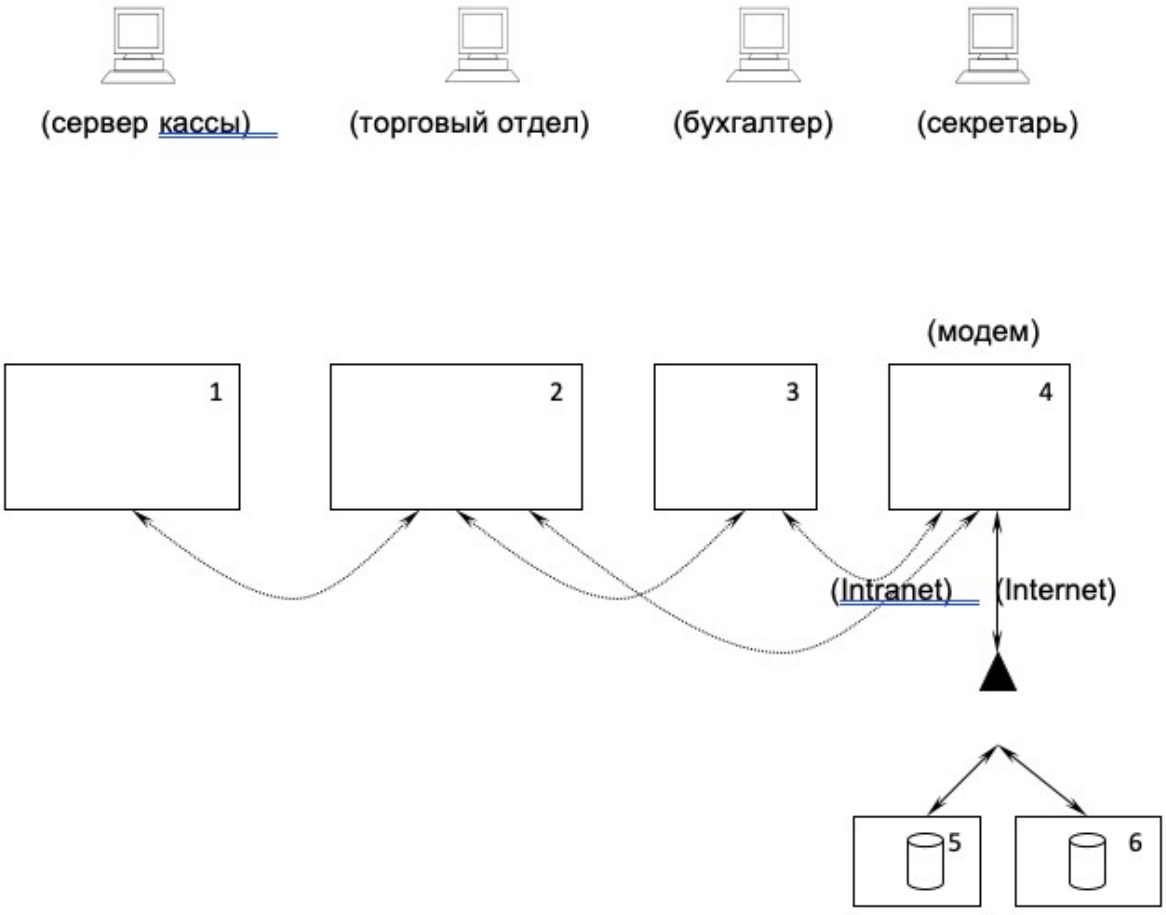

Рисунок 10. Существующая информационная модель предприятия

В таблице 1 используя документооборот предприятия, составим подробное описание информационных потоков на базе имеющихся источников информации и получателей с указанием характера передаваемой информации.

Таблица 1

Информационные потоки

Код потока	**Источник информации**	**Получатель информации**	**Характер информации**
1	**2**	**3**	**4**
1/2	сервер кассы	торговый отдел	Товарные чеки, налоговые накладные
1/3	сервер кассы	бухгалтер	-
1/4	сервер кассы	секретарь	-

1	**2**	**3**	**4**
1/5	сервер кассы	Intranet	-
1/6	сервер кассы	Internet	-
2/1	торговый отдел	сервер кассы	Товарные остатки, цены
3/1	бухгалтер	сервер кассы	-
4/1	секретарь	сервер кассы	-
5/1	Intranet	сервер кассы	-
6/1	Internet	сервер кассы	-
2/3	торговый отдел	бухгалтер	Отчеты о продажах по кассе, расходные накладные, приходные накладные, реестр налоговых накладных, товарные остатки подразделения
2/4	торговый отдел	секретарь	Маркетинговые отчеты
2/5	торговый отдел	Intranet	Маркетинговые отчеты, товарные остатки подразделения, возвратные накладные, заявки-заказы
2/6	торговый отдел	Internet	Деловая переписка
3/2	бухгалтер	торговый отдел	Распоряжения по ценообразованию и проведению инвентаризаций
4/2	секретарь	торговый отдел	Распоряжения, приказы
5/2	Intranet	торговый отдел	Товарные остатки головного предприятия, расходные накладные головного предприятия
6/2	Internet	торговый отдел	Деловая переписка, коммерческая информация для проведения анализа рынка и товаров
3/4	бухгалтер	секретарь	Отчеты о деятельности подразделения

1	2	3	4
3/5	бухгалтер	Intranet	Бухгалтерская отчетность для головного предприятия
3/6	бухгалтер	Internet	Деловая переписка
4/3	секретарь	бухгалтер	Распоряжения, приказы
5/3	Intranet	бухгалтер	Бухгалтерская отчетность головного предприятия
6/3	Internet	бухгалтер	Деловая переписка
4/5	секретарь	Intranet	-
4/6	секретарь	Internet	Деловая переписка
5/4	Intranet	секретарь	-
6/4	Internet	секретарь	Деловая переписка, распоряжения головного предприятия

Внешними информационными потоками в данной структуре являются потоки информации, поступающие из Intranet, этот источник представляет собой связь посредством модема с локальной сетью головного предприятия. Данный подход обмена информацией дает возможность передавать информацию, имеющую статус коммерческой тайны, по мере необходимости и с максимальной защищенностью, и сократить расходы связи, так как стоимость выделенной линии в Internet является дорогостоящим удовольствием.

Так же Internet является внешним информационным потоком, здесь используется система online, т.е. почтовый сервер. Смысл такого подхода заключается в том, что почта передается не зависимо от состояния междугородней связи. Почта выгружается на сервер провайдера по городской телефонной линии, а далее без участия отправителя доставляется в почтовый ящик получателя, это весьма эффективно в условиях существующего качества телефонной связи, так как отправка почтового пакета занимает очень мало времени. Этот подход позволяет сократить расходы на Internet и получить весьма эффективный канал связи в свое распоряжение.

Анализируя данные таблицы 1. составим более универсальную структуру информационной модели предприятия. (рисунок 11)

Полученная совокупность информационных потоков послужит основой для разработки локальной информационной сети подразделения, с целью повышения эффективности управленческого процесса.

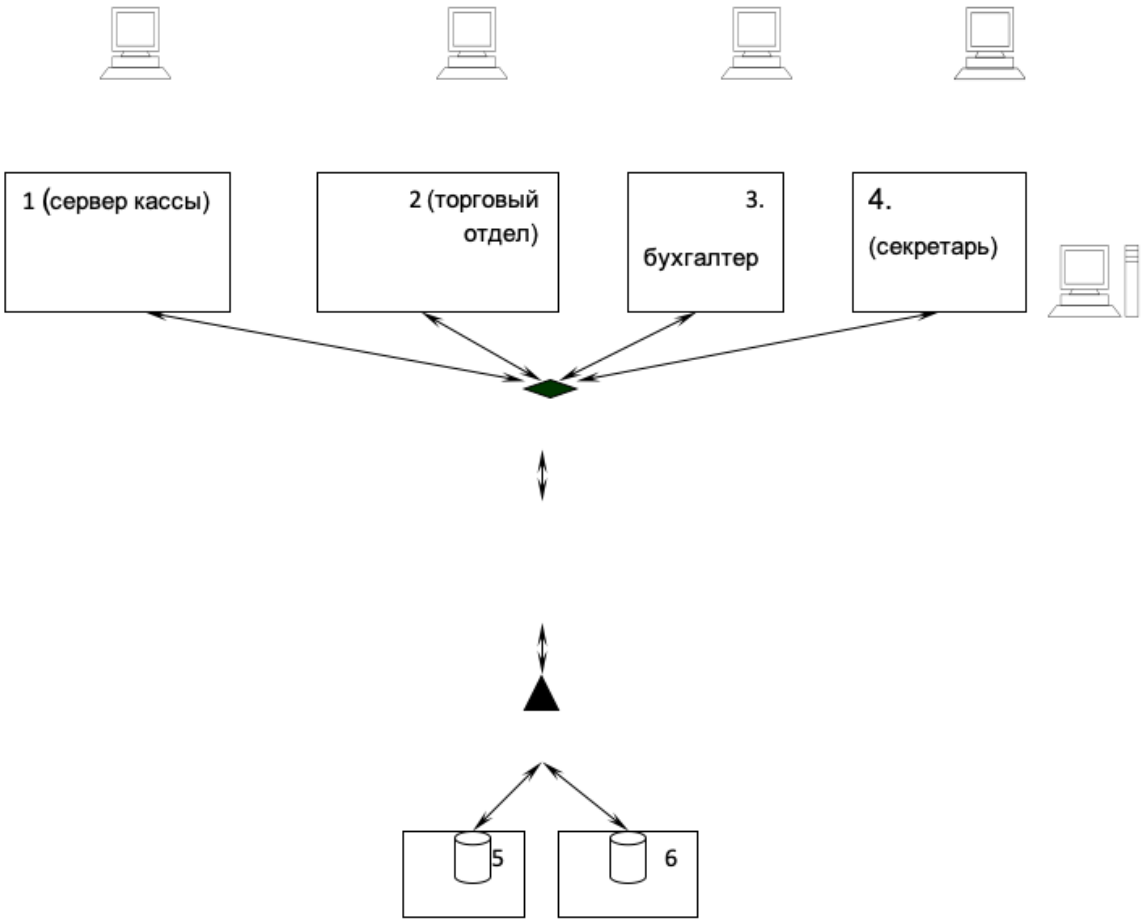

Рисунок 11. Разработанная информационная модель предприятия

3.2 Характеристика решаемых управленческих задач

Использование локальной компьютерной сети на предприятии позволяет сократить бумажный документооборот, имеющийся на предприятии, повысить производительность труда, сократить время на обработку информации, что существенно влияет на качество выполнения управленческих задач.

На выбранном предприятии, работы по созданию и внедрению информационной системы выполняются в условиях наличия разрозненной компьютерной техники, используемой каждым отделом самостоятельно.

На предприятии принято решение о создании единой информационной системы с целью организации оперативного и эффективного учета товарно-материальных ценностей, проведения оперативного бухгалтерского учета, маркетингового анализа и интеграции бухгалтерской отчетности подразделения в бухгалтерский учет головного предприятия.



Рисунок 12. Дерево целей

Внедрение компьютерной информационной системы на предприятии направленно на эффективное решение ряда управленческих задач (на рисунке 12 приведено дерево целей):

1) управление материально-техническим снабжением, т.е. осуществлять своевременное и комплексное обеспечение потребностей предприятия в товаре;
2) управление сбытом, т.е. проводить оперативное управление реализацией товара, на основе оперативного учета сбыта, прогнозирования спроса, структуры реализации и прибыли;
3) технико-экономическое планирование – комплекс расчетов, основное назначение которых — это обоснование рациональных объемов закупки, ассортимента, разработки эффективных методик реализации товара и создания предпосылок для эффективной деятельности персонала.

3.3 Выбор и описание локальной компьютерной сети

В штатной структуре предприятия имеется четыре отдела, самостоятельно выполняющие функции учета и оперативного управления. Они и послужат основой структуры будущей локальной информационной системы подразделения.

Каждая структурная единица имеет минимальное необходимое оборудование, т.е. процесс внедрения сети будет заключаться в объединении имеющейся оргтехники на основе выбранной оптимальной типологий сети. В таблице 2 приведен состав имеющейся оргтехники по каждой структурной единице.

Таблица 2

Имеющаяся оргтехника подразделений

Название отдела	**Наименование оргтехники**	**Количество, шт.**
1	**2**	**3**
Торговый зал	Касса	1
	Компьютер	1
Торговый отдел	Компьютер	1
	Принтер	1
Бухгалтерия	Компьютер	1

	Принтер	1
Секретарь	Компьютер	1
	Принтер	1
	Модем	1

Четко представляя информационную структуру предприятия, перейдем к рассмотрению вопроса выбора наиболее эффективного типа сети.

Наиболее эффективной будет сеть в виде «звезда» на основе сервера. Ее преимущество в том, что:

1) сервер обеспечивает высокопроизводительную обработку запросов клиентов;
2) обеспечивает работу компьютеров отделов в качестве клиента сети;
3) внутренние вычисления клиентов не влияют на скорость процессора сервера;
4) поломка клиента не влияет на работу всей сети;
5) имеется единое лицо отвечающие за администрирование ресурсов сети;
6) обеспечивает возможность ограничения и контроля доступа к сетевым ресурсам;
7) устанавливаемый на сервер брэндмауэр, защищает локальную сеть от доступа через внешние каналы связи;
8) при выходе из строя сервера, имеется возможность замкнуть сеть в «звезду» без сервера (что правда скажется на производительности сети) или «шину».

Из всего множества имеющихся видов сетевого кабеля, наиболее эффективным будет использование экранированной витой пары, ее преимущества в том, что:

1) низкая стоимость;
2) высокая помехозащищенность;
3) высокая производительность в скорости передачи данных;

4) простата установки;
5) размеры площадей позволяют уложиться в минимальную эффективную длину кабеля.

Сетевые платы необходимы с поддержкой подключения витой пары, желательно известных производителей с целью их высокой надежности и возможностью обновления драйверов для этих плат.

Также необходимо установит на кассу адаптер для автоматической регистрации компьютером продаваемого товара, что позволит производить автоматическое списание проданного через кассу товара с остатков в режиме реального времени, т.е. остатки предприятия будут соответствовать действительности после пробития чека по кассе.

Сопоставляя имеющуюся оргтехнику с разработанной информационной моделью (рисунок 11) и выбранного типа сети, определим недостающие оборудование для построения законченной структуры локальной информационной системы, таблица 3.

Таблица 3

Необходимое оборудование

Наименование оргтехники	**Количество, шт.**
1	**2**
Сервер	1
Концентратор	1
Адаптер для кассы	1
Сетевая плата	4
Сетевой кабель	Количество определяется схемой размещения оргтехники и планом помещений предприятия

3.4 Сетевое программное обеспечение ООО «АйТиЭл»

В качестве основной операционной системы сети подразделения, предполагается использование ОС Windows 10 встроенные возможности этой ОС позволяют реализовать: организацию локальной сети, взаимодействие с

другими операционными системами и интегрировать в сеть, встроенные в эту операционную систему, технологии Internet, защиту информации от несанкционированного доступа. Использование ОС Windows 10 также позволяет применять в работе пользователей сети весь спектр программного обеспечения, производимого корпорацией Microsoft.

В состав операционной системы Windows 10 входят все программные продукты необходимые для организации и эксплуатации сети:

1) транспортные протоколы NetBEUI, IPX/SPX, TCP/IP;
2) сервер IIS;
3) Internet Explorer – интернет браузер;
4) Outlook Express – почтовый клиент;
5) Route, Netwatch и Winipcfg – программы маршрутизации, администрирования и конфигурирования сети;
6) Web Publish и FrontPage – программы организации локального Intranet-а и сайтов;
7) Wscript – сервер сценариев.

На всех имеющихся компьютерах предприятия уже установлена операционная система Windows 10, что позволит сократить расходы на внедрение новой операционной системы.

3.5 Пользовательское программное обеспечение. Построение схемы сети

Как указывалось выше, операционная система позволяет использовать все программные продукты корпорации Microsoft, но нас более всего интересует пакет Microsoft Office.

Программный пакет Microsoft Office, данной корпорации, позволяет решать все задачи, связанные с организацией учета, оперативным планированием, организацией и ведением документооборота. Программы этого пакета имеют высокую степень интеллектуальности и полностью интегрированы с сетевыми технологиями, технологиями безопасности

информации, также программы имеют полную внутреннею совместимость на уровне протоколов обмена данными, что очень важно при создании сложных систем обработки информации (взаимодействие текстовых документов, электронных таблиц и баз данных между собой).

Также, привлекательным является тот факт, что корпорация Microsoft поддерживает открытую архитектуру программного обеспечения и с использованием прикладного пакета Visual studio, производимого этой же корпорацией, появляется возможность на уровне программирования производить настройку существующих программ по критериям конкретной решаемой задачи.

В состав пакета входят такие программы как:

1) Microsoft Access – организация и управление базами данных;
2) SQL Server – сервер управления базами данных;
3) Microsoft Word – текстовый редактор;
4) Microsoft Excel – электронные таблицы;
5) Microsoft Expert – система анализа.

Для организации учета, будет использоваться система СКАТ использующая систему баз данных Microsoft Access. Эта система позволяет вести приходные и расходные документы, товарные чеки, налоговые накладные, товарные остатки и различные отчеты для оперативного планирования и прогнозирования. Система СКАТ позволяет интегрировать имеющуюся информацию в систему бухгалтерского учета 1С Бухгалтерия. 1С Бухгалтерия позволяет вести оперативные бухгалтерский учет.

Данный пакет и 1С Бухгалтерия также установлены на компьютерах предприятия, что также позволит сократить расходы на приобретение и внедрение программного обеспечения необходимого для организации учета и эффективного управления предприятием.

4 АНАЛИЗ ЗАТРАТ НА ОРГАНИЗАЦИЮ И ОБСЛУЖИВАНИЕ ЛОКАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ И ЭФФЕКТИВНОСТИ СИСТЕМЫ БЕЗОПАСНОСТИ

Фирма понесет затраты на приобретение недостающего для организации локальной информационной сети оборудования и программного обеспечения, в таблицах 4 и 5 приведен расчет необходимых денежных средств.

Таблица 4

Расчет затрат на приобретение оборудования

Наименование оргтехники	**Количество, шт.**	**Цена за ед., руб.**	**Сумма, руб.**
1	**2**	**3**	**4**
Сервер	1	45833	45833
Концентратор	1	1146	1146
Адаптер для кассы	1	688	688
Сетевая плата	4	275	1100
Сетевой кабель	200 м.п.	5	1000
Система СКАТ	на 5 клиентов	5730	28650
		Итого:	78417

Таблица 5

Стоимость услуг

Наименование оргтехники	**Количество**	**Цена за ед., руб.**	**Сумма, руб.**
1	**2**	**3**	**4**
Прокладка и настройка сети		25000	25000
Обучение персонала	5 человек	417	2085
Абонентская плата по обслуживанию	1 месяц	62	341
		Итого:	27426

Общая стоимость внедрения сети составит 105843 рубля.

Произведем расчет эффективности от внедрения ЛВС:

$$C\acute{y} = \sum_{i=1}^{7} Ci^{\acute{y}}$$, где

$Ci^э$ - основная и дополнительная зарплата с отчислениями на соцстрах (принимается равным 6% от суммы основной и дополнительной зарплаты),

- амортизация, ремонт (3-4% от стоимости ТС),

- затраты на аренду КС, прочие расходы (принимаются в размере 0,7

- 1% от стоимости ТС варианта КТС).

Заработная плата - 40840 руб. * 6% = 2450 руб.

40840 – 2450 = 38390 руб.

Амортизация основных фондов = 12688 руб.

Электроэнергия = 530 руб.

Ремонт = 3167 руб.

Прочие = 1058 руб.

$С_э$ = 58283 руб.

Затраты на приобретение средств ВТ для одного АРМ:

$К_{ивс}$ = К1 + К2 + К3, где

К1 - производственные затраты;

К2 - капитальные вложения;

К3 - остаточная стоимость ликвидированного оборудования.

$$æ2 = \sum_{i=1}^{6} Ki^k$$, где

Ki - затраты на приобретение ЭВМ, АП, Т, помещений, прокладку КС, служебных площадей и т.д.

$$æ3 = \sum_{i=1}^{m} Ki^b\left(1-\alpha\, Ti^{ý}\right)$$, где

Ki^b - первоначальная стоимость действующего i - го вида оборудования;

α - годовая норма амортизации (12% от стоимости ТС);

$Ti^э$ - длительность эксплуатации i - го вида оборудования.

$К_э$ = 105843(1-0,12*5) = 42337 руб.

K_2 = 105843 руб.

$K_{ивс}$= 105843+42337+20833 = 169013 руб.

Затраты на приобретение средств ВТ для одного АРМ:

$$R = \frac{æ\blacksquare \quad /Ò \quad + (ý + (}{N}$$, где

Кивс - общие затраты на проектирование и создание ИВС;

Тн - нормативный срок жизненного цикла технического обеспечения (6 -8 лет);

Сэ - текущие ежегодные эксплуатационные расходы;

Сn - текущие ежегодные расходы на развитие программных средств.

R = 5067 руб.

Ежегодный экономический эффект определяется по формуле:

$$H = \frac{X * K * C * (P - 100)}{100}$$, где

X - число ИТР и служащих, пользующихся одним АРМ (обычно 2-4);

K - средневзвешенное число смен (1 - 2,5);

C - средние ежегодные затраты на одного сотрудника;

P - относительная средняя производительность сотрудника, пользующегося АРМом (140 - 350%).

H = 3458*250/100 = 8645 руб.

Экономические эффект от внедрения одного АРМ

Z = H - R, где

H - ежегодный экономический эффект;

R - приведенные к одному АРМ затраты на приобретение средств ВТ и системы передачи данных и т.д.

Z = 8645 – 5067 = 3578 руб.

Годовая экономия от внедрения ЛВС определяется по формуле:

Э = N * Z, где

N - количество автоматизированных рабочих мест (АРМ);

Z - прямой экономический эффект от внедрения одного АРМ.

Э = 4*3578 = 14312 руб.

Срок окупаемости:

169013/14312 = 12 месяцев

Выводы:

1) внедрение ЛВС целесообразно;
2) срок окупаемости составит 1 год.

На данный момент получены следующие результаты:

1) спроектирована, смонтирована и введена в эксплуатацию исследуемая корпоративная сеть;
2) намечены мероприятия по организации информационной безопасности.

Планируется получение математической модели универсальной корпоративной сети, оснащенной современными средствами защиты от внешних и внутренних угроз, которая могла бы удовлетворить самым требовательным запросам.

Проектирование сети проходило в следующем порядке:

1) Сделан выбор среды передачи. Проведенные исследования возможных сред передачи (витая пара, оптоволокно, беспроводные технологии) показали, что оптоволокно обладает наилучшими показателями по надежности, скорости и помехозащищенности. В качестве среды передачи был выбран одномодовый оптоволоконный кабель.

2) Сделан выбор топологии сети. Были проанализированы различные топологии (звезда, кольцо, общая шина), и в качестве физической выбрана гибридная топология двойное кольцо, а в качестве логической – топология звезда. Для большей надежности проброшен линк от крайнего узла сети в центральный.

3) Выбрана технология передачи. Технология Gigabit Ethernet отвечает всем требованиям по скорости и надежности передачи. Эта технология является наиболее распространенной и поддерживается оборудованием всех

производителей. Но в этом есть и свои недостатки: чем популярнее технология, тем легче злоумышленнику организовать вторжение или нарушить работу сети. Для предотвращения вторжения необходимо правильно подобрать средства защиты периметра сети, а также продумать комплекс мер по защите от внутренних угроз.

4) Выбраны активные компоненты сети. В качестве вендора выбрана фирма Cisco Systems, т.к. они предлагают комплексный подход к организации сетей различной степени сложности.

Для организации подсистемы защиты выбраны следующие основные средства:

1) Средства разграничения доступа. Будут организованы виртуальные локальные сети (VLAN). Кроме того, будут настроены права доступа индивидуально каждому работнику (рисунок 13).

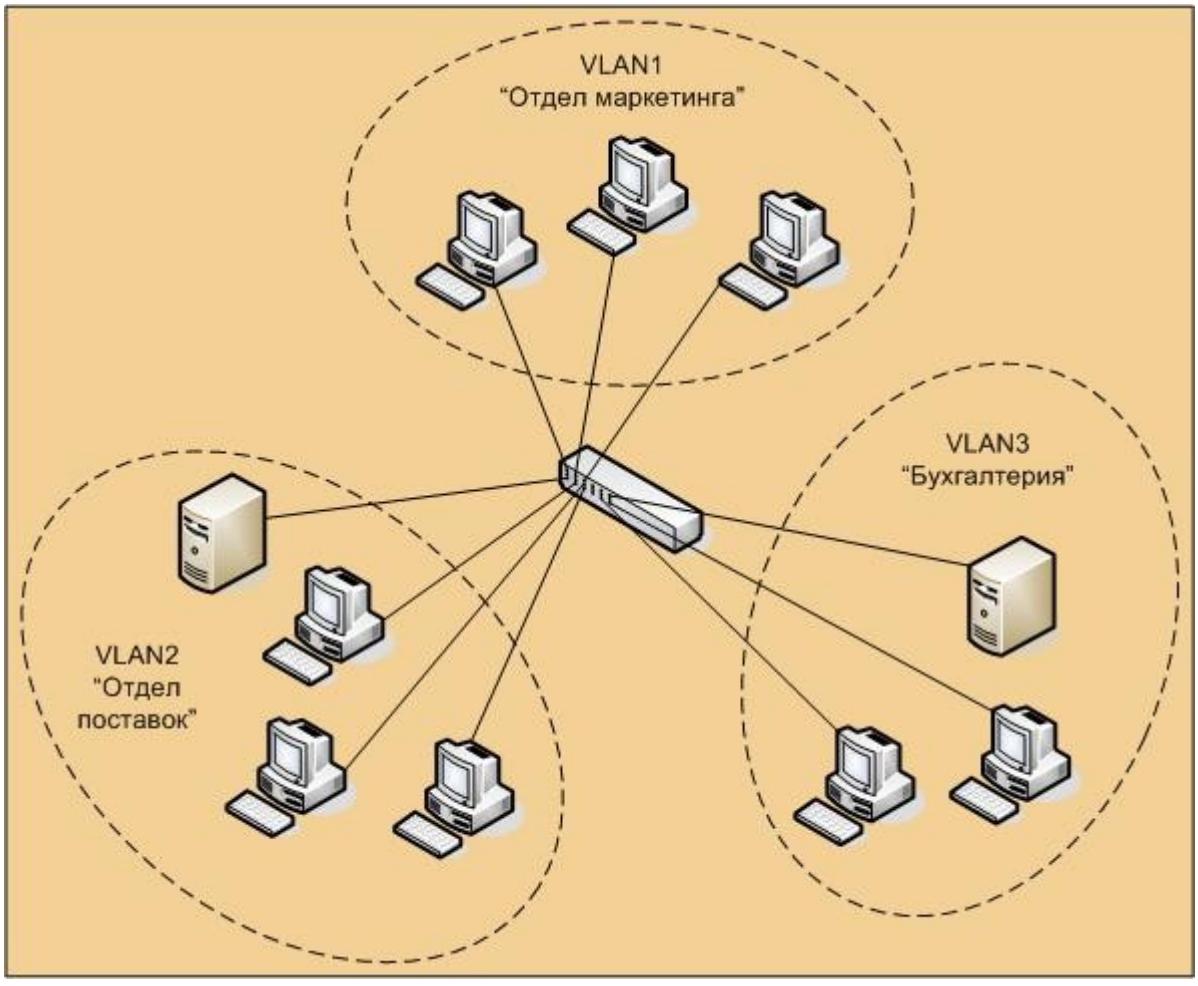

Рисунок 13. Организация виртуальных локальных сетей

2) Установка межсетевых экранов. Firewall (брендмауэр) будет установлен на границе между внутренней сетью и Интернет для противодействия несанкционированному межсетевому доступу.

3) Система обнаружения вторжений Intrusion Detection System, IDS - служит для обнаружения попыток несанкционированного доступа путем фонового сканирования трафика.

4) Защита информация при передаче по каналам связи, которые не контролируются или контролируются лишь частично (например - Интернет). Распространенные способы защиты - криптография, физические средства защиты.

5) Системы идентификации, аутентификации и авторизации.

Идентификация – процедура предоставления субъектом (пользователем, компьютером) своего уникального идентификатора

Аутентификация – процедура подтверждения субъектом предоставленного идентификатора

Авторизация – процедура определения прав доступа субъекта

Способы аутентификации:

1) программные;
2) парольные;
3) аппаратно-программные;
4) с предоставлением уникального идентификатора (смарт-карты, token);
5) биометрические (отпечатки пальцев, радужная оборочка глаза);

6) организация системы поиска уязвимостей следующими путями:

- √ выявление уязвимостей путем:
  - √ анализа настроек (пассивный поиск);
  - √ имитацией атак (активный поиск).
- √ область сканирования:
  - √ сетевой сканер;
  - √ системный сканер;

- √ сканер уязвимости приложений (СУБД, WEB-сервер).

√ результат сканирования:

- √ выдача списка уязвимостей;
- √ выдача рекомендаций (экспертные системы);
- √ устранение уязвимостей в автоматическом/полуавтоматическом режиме.

7) Антивирусная защита. Для защиты сети от всевозможных вредоносных программ, червей и спама наряду с техническими средствами (активное оборудование фирмы Cisco Systems имеет функции обнаружения вредоносного кода) используются стандартные антивирусные программы.

При создании математической модели надежной и безопасной корпоративной сети использована реальная сеть предприятия ООО «АйТиЭл». На ее примере рассмотрены аспекты технической надежности топологии сети, а также аспекты информационной безопасности корпоративной сети предприятия.

Будет выбран комплекс средств по организации средств защиты.

Для самого предприятия ООО «АйТиЭл» данная разработка будет важным шагом по автоматизации процесса производства и по защите конфиденциальной информации от злоумышленников.

Кроме того, данная модель может быть использована для определения степени защищенности любого предприятия, а также для организации подсистемы защиты информации на предприятии.

Задача оценки эффективности контрмер является не менее сложной, чем оценка рисков.

Причина в том, что оценка эффективности комплексной подсистемы безопасности, включающей контрмеры разных уровней (административные, организационные, программно-технические), в конкретной информационной системе – методологически чрезвычайно сложная задача. По этой причине обычно используются упрощенные, качественные оценки эффективности контрмер.

Примером является следующая таблица типичных значений эффективности контрмер, применяемых в методе анализа рисков RiskWatch.

Таблица 6

Ориентировочная эффективность мероприятий в области защиты информации по критерию ROI (Return of Investment – возврат вложений)

Мероприятие	**Оценка**
1	**2**
Разработка и внедрение политики информационной безопасности	2
Мероприятия по работе с персоналом (наведение справок, контроль за поведением и т. п.)	3
Совершенствование организационной структуры	4
Анализ рисков	5
Управление жизненным циклом (управление рисками)	5
Совершенствование должностных инструкций и условий контрактов	5
Меры контроля за посетителями	6
Управление имуществом компании	7
Обучение персонала и контроль за соблюдением режима ИБ	9
Меры контроля за работой приложений	10

Указанные в таблице значения являются ориентировочными оценками эффективности вложений в различные классы мероприятий в области защиты информации.

В ряде случаев используются более сложные таблицы, в которых эффективность зависит от определенных факторов. На основе подобных таблиц делаются качественные оценки эффективности контрмер.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности компании. При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств

защиты могут быть определены как количественными методами (например, при определении стоимостных характеристик), так и качественными (например, учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды). Таким образом, анализ и управление информационными рисками позволяет обеспечить экономически оправданную безопасность компании.

ЗАКЛЮЧЕНИЕ

Анализ и управление информационными рисками позволяет обеспечивать экономически оправданную информационную безопасность в любой отечественной компании. Для этого необходимо сначала определить, какие информационные активы компании нужно защищать, воздействию каких угроз эти активы подвержены, а затем выработать рекомендации по защите данных.

В любой методике управления рисками необходимо идентифицировать риски, как вариант – их составляющие (угрозы и уязвимости). Естественное требование к списку — его полнота. Сложность задачи составления списка и доказательство его полноты зависит от того, какие требования предъявляются к детализации списка. На базовом уровне безопасности, как правило, не предъявляется специальных требований к детализации классов и достаточно использовать какой-либо подходящий в данном случае стандартный список классов рисков. Оценка величины рисков не рассматривается, что приемлемо для отдельных методик базового уровня. Списки классов рисков содержатся в некоторых руководствах, в специализированном ПО анализа рисков. Примером является немецкий стандарт BSI (www.bsi.de, — в нем имеется каталог угроз применительно к различным элементам информационной технологии.

При оценивании рисков рекомендуется рассматривать следующие аспекты:

- √ шкалы и критерии, по которым можно измерять риски;
- √ оценка вероятностей событий;
- √ технологии измерения рисков.

Обеспечение безопасности сети требует постоянной работы и пристального внимания к деталям. Эта работа заключается в предсказании возможных действий злоумышленников, планировании мер защиты и постоянном обучении пользователей. Если же вторжение состоялось, то

администратор безопасности должен обнаружить брешь в системе защиты, ее причину и метод вторжения

Формируя политику обеспечения безопасности, администратор прежде всего проводит инвентаризацию ресурсов, защита которых планируется; идентифицирует пользователей, которым требуется доступ к каждому из этих ресурсов, и выясняет наиболее вероятные источники опасности для каждого из этих ресурсов. Имея эту информацию, можно приступать к построению политики обеспечения безопасности, которую пользователи будут обязаны выполнять.

Политика обеспечения безопасности — это не обычные правила, которые и так всем понятны. Она должна быть представлена в форме серьезного печатного документа. А чтобы постоянно напоминать пользователям о важности обеспечения безопасности, можно разослать копии этого документа по всему офису, чтобы эти правила всегда были перед глазами сотрудников.

Хорошая политика обеспечения безопасности включает несколько элементов, в том числе следующие:

- √ Оценка риска. Что именно мы защищаем и от кого? Нужно идентифицировать ценности, находящиеся в сети, и возможные источники проблем;
- √ Ответственность. Необходимо указать ответственных за принятие тех или иных мер по обеспечению безопасности, начиная от утверждения новых учетных записей и заканчивая расследованием нарушений;
- √ Правила использования сетевых ресурсов. В политике должно быть прямо сказано, что пользователи не имеют права употреблять информацию не по назначению, использовать сеть в личных целях, а также намеренно причинять ущерб сети или размещенной в ней информации;

- √ Юридические аспекты. Необходимо проконсультироваться с юристом и выяснить все вопросы, которые могут иметь отношение к хранящейся или генерируемой в сети информации, и включить эти сведения в документы по обеспечению безопасности;
- √ Процедуры по восстановлению системы защиты. Следует указать, что должно быть сделано в случае нарушения системы защиты и какие действия будут предприняты против тех, кто стал причиной такого нарушения.

В данной работе были рассмотрены вопросы организации локальных информационных систем в разрезе деятельности коммерческого предприятия.

В частности, были рассмотрены такие важные и интересные вопросы, как удаленный доступ к сети, подключение локальных информационных систем к глобальным сетям типа Internet, технология защиты сетей от несанкционированного использования информации и роль информационных сетей в процессе управления предприятием и повышения эффективности управленческого процесса.

Рассмотренные вопросы представляют большой интерес. На сегодняшний день разработка и внедрение локальных информационных систем является одной из самых интересных и важных задач в области информационных технологий. Все больше возрастает стоимость информации и зависимость предприятий от оперативной и достоверной информации. В связи с этим появляется потребность в использовании новейших технологии передачи информации. Сетевые технологии очень быстро развиваются, в связи с чем они начинают выделяться в отдельную информационную отрасль. Ученные прогнозируют, что ближайшим достижением этой отрасли будет полное вытеснение других средств передачи информации (телевидение, радио, печать, телефон и т.д.). На смену этим «устаревшим» технологиям придет компьютер, он будет подключен к некоему глобальному потоку

информации, и из этого потока можно будет получить любую информацию в любом представлении.

Ведь интенсивное использование информационных технологий уже сейчас является сильнейшим аргументом в конкурентной борьбе, развернувшейся на мировом рынке.

В качестве предложения по повышению политики корпоративной безопасности можем предложить следующий образец.

Образец политики корпоративной безопасности

Цель: гарантировать использование по назначению компьютеров и телекоммуникационных ресурсов Компании ее сотрудниками, независимыми подрядчиками и другими пользователями. Все пользователи компьютеров обязаны использовать компьютерные ресурсы квалифицированно, эффективно, придерживаясь норм этики и соблюдая законы.

Следующая политика, ее правила и условия касаются всех пользователей компьютерных и телекоммуникационных ресурсов и служб компании, где бы эти пользователи ни находились. Нарушения этой политики влечет за собой дисциплинарные воздействия, вплоть до увольнения и/или возбуждения уголовного дела.

Данная политика может периодически изменяться и пересматриваться по мере необходимости.

Руководство компании имеет право, но не обязано проверять любой или все аспекты компьютерной системы, в том числе электронную почту, с целью гарантировать соблюдение данной политики. Компьютеры и бюджеты предоставляются сотрудникам Компании с целью помочь им более эффективно выполнять свою работу.

Компьютерная и телекоммуникационная системы принадлежат Компании и могут использоваться только в рабочих целях. Сотрудники Компании не должны рассчитывать на конфиденциальность информации, которую они создают, посылают или получают с помощью принадлежащих Компании компьютеров и телекоммуникационных ресурсов.

Пользователям компьютеров следует руководствоваться перечисленными ниже мерами предосторожности в отношении всех компьютерных и телекоммуникационных ресурсов и служб. Компьютерные и телекоммуникационные ресурсы и службы включают в себя (но не ограничиваются) следующее: хост-компьютеры, серверы файлов, рабочие станции, автономные компьютеры, мобильные компьютеры, программное обеспечение, а также внутренние и внешние сети связи (интернет, коммерческие интерактивные службы и системы электронной почты), к которым прямо или косвенно обращаются компьютерные устройства Компании.

Пользователи должны соблюдать условия всех программных лицензий, авторское право и законы, касающиеся интеллектуальной собственности.

Неверные, навязчивые, непристойные, клеветнические, оскорбительные, угрожающие или противозаконные материалы запрещается пересылать по электронной почте или с помощью других средств электронной связи, а также отображать и хранить их на компьютерах Компании. Пользователи, заметившие или получившие подобные материалы, должны сразу сообщить об этом инциденте своему руководителю.

Все, что создано на компьютере, в том числе сообщения электронной почты и другие электронные документы, может быть проанализировано руководством Компании.

Пользователям не разрешается устанавливать на компьютерах и в сети Компании программное обеспечение без разрешения системного администратора.

Пользователи не должны пересылать электронную почту другим лицам и организациям без разрешения отправителя.

Электронная почта от юриста Компании или представляющего ее адвоката должна содержать в колонтитуле каждой страницы сообщение: "Защищено адвокатским правом/без разрешения не пересылать".

Пользователям запрещается изменять и копировать файлы, принадлежащие другим пользователям, без разрешения владельцев файлов.

Запрещается использование без предварительного письменного разрешения компьютерных и телекоммуникационных ресурсов и служб Компании для передачи или хранения коммерческих либо личных объявлений, ходатайств, рекламных материалов, а также разрушительных программ (вирусов и/или самовоспроизводящегося кода), политических материалов и любой другой информации, на работу с которой у пользователя нет полномочий или предназначенной для личного использования.

Пользователь несет ответственность за сохранность своих паролей для входа в систему. Запрещается распечатывать, хранить в сети или передавать другим лицам индивидуальные пароли. Пользователи несут ответственность за все транзакции, которые кто-либо совершит с помощью их пароля.

Возможность входа в другие компьютерные системы через сеть не дает пользователям права на подключение к этим системам и на использование их без специального разрешения операторов этих систем.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Абрамов В.А. «Введение в теорию систем детерминированного, стохастического и нечеткого типа». МИЭТ.- Москва, 2016.
2. Аккорд 1.95. Описание применения. 1143195.4012-003 31, ОКБ САПР.- Москва, 2016.
3. Баутов А. Стандарты и оценка эффективности защиты информации. Доклад на Третьей Всероссийской практической конференции "Стандарты в проектах современных информационных систем".- Москва, 23-24 апреля 2018 г.
4. Баутов А., Экономический взгляд на проблемы информационной безопасности. //Открытые системы.- 2002.- № 2. –с.12-23
5. Валда Хиллей. Секреты Windows NT Server 4.0./ – К.: Диалектика, 2017.
6. Виноградов С.М. и др. Информационное общество: Информационные войны. Информационное управление. Информационная безопасность. Изд. СПбУ, 2016.
7. Вихорев С., А. Ефимов, Практические рекомендации по информационной безопасности. Jet Info, № 10-11, 2016.
8. Вихорев С., Р. Кобцев, Как определить источники угроз.// Открытые системы.- 2018.- № 7-8. –с.9-16
9. Галатенко В.А., Информационная безопасность - основы. Системы управления базами данных, 2016, № 1.
10. Галатенко В.А. Основы информационной безопасности Интернет-университет информационных технологий - ИНТУИТ.ру, 2018
11. Галатенко В.А. Стандарты информационной безопасности Интернет-университет информационных технологий - ИНТУИТ.ру, 2017.
12. Герасименко В.А. Проблемы защиты данных в системах их обработки.// Зарубежная радиоэлектроника.- №12.- 2017

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ А

Схема разработанной локальной информационной сети, внедряемой на предприятии ООО «АйТиЭл»

