Т.А. Биячуев

Безопасность Корпоративных Сетей

под редакцией
Л. Г. Осовецкого

Учебное пособие

2004

Министерство образования и науки Российской Федерации

**Санкт-Петербургский государственный
университет информационных технологий,
механики и оптики**

Кафедра безопасных информационных технологий

Т.А. Биячуев

БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ СЕТЕЙ

Под редакцией Л.Г. Осовецкого

Учебное пособие

Санкт-Петербург
2004

УДК 621.394

Биячуев Т.А. / под ред. Л.Г.Осовецкого Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004.- 161 с.

Настоящее учебно-методическое пособие посвящено актуальным вопросам построения защищенных корпоративных сетей. Особое внимание уделено математическому моделированию корпоративных сетей, вопросам построения комплексных систем защиты информации с гарантиями по безопасности, методам и средствам защиты от внутренних нарушителей в корпоративных сетях.

Обсуждаются проблемы безопасности корпоративных сетей современных предприятий, научно-технические принципы построения систем обеспечения безопасности информационных ресурсов корпоративных сетей с учетом современных тенденций развития сетевых информационных технологий, методы и средства анализа защищенности корпоративных сетей, технологии межсетевого экранирования, системы обнаружения вторжений и средства построения виртуальных частных сетей.

Подробно описываются угрозы, исходящие от внутренних нарушителей корпоративных сетей. На основе моделирования действий внутренних нарушителей, предложены методы защиты и рекомендации по усилению общей защищенности корпоративных сетей.

При подготовке издания использовались материалы, как отечественных авторов – Л.Г. Осовецкого, А.В. Лукацкого, А.А. Астахова, А.А. Молдовяна, А.В. Соколова, В.Ф. Шаньгина, И.Д. Медведковского и др., так и зарубежных специалистов – M. Howard, R. Graham, D. Sanai, S. Manwani, M. Montoro, Z. Shuanglei, K. Kasslin, A. Tikkanen, а также других экспертов в области сетевой безопасности.

Пособие рассчитано на специалистов, администраторов компьютерных сетей и систем, студентов старших курсов и аспирантов соответствующих специальностей, а также всех заинтересованных проблемами обеспечения информационной безопасности корпоративных сетей.

УДК 621.394

Оглавление

Термины и определения

АРМ – автоматизированное рабочее место
АС – автоматизированная система
АСОД – автоматизированная система обработки данных
ГВС – глобальная вычислительная сеть
ЗИ – защита информации
ИБ – информационная безопасность
ИТ – информационные технологии
КС – корпоративная сеть
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ к информации
ОС – операционная система
ПО – программное обеспечение
РД – руководящий документ
СВТ – средства вычислительной техники
СЗИ – система защиты информации
СКД – система контроля доступа
СОА – система обнаружения атак
СОБИ КС – система обеспечения безопасности информационных ресурсов корпоративных сетей
СПД ОП – система передачи данных общего пользования
СУБД – система управления базами данных
ТКС – телекоммуникационные сети
ЭМВОС – эталонная модель взаимодействия открытых систем

Корпоративная информационная система (сеть) - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Уязвимость – это присущие объекту причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.

Угроза – это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику или пользователю, проявляющегося в опасности искажения, раскрытия или потери информации.

Атака – это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся факторы (уязвимости).
Нарушитель – лицо, по ошибке, незнанию или осознанно предпринявшее попытку выполнения запрещенных операций и использующее для этого различные возможности, методы и средства.

Введение

В настоящем методическом пособии представлены научно-технические принципы построения систем обеспечения безопасности информационных ресурсов корпоративных сетей (СОБИ КС) с учетом современных тенденций развития сетевых информационных технологий. Рассмотрены современные технологии, используемые для построения защищенных корпоративных сетей, исследованы методы защиты от внутренних нарушителей. Предлагаемое пособие состоит из трех разделов.

В первом разделе рассматриваются элементы математической модели корпоративной сети, предложенной в работах Осовецкого Л.Г., Твердого Л.В, Немолочнова О.Ф. [1].

Построение современных СОБИ КС основывается на комплексном подходе, доказавшем свою эффективность и надежность. Комплексный подход ориентирован на создание защищенной среды обработки информации в корпоративных системах, сводящей воедино разнородные меры противодействия угрозам. Сюда относятся правовые, морально-этические, организационные, программные и технические способы обеспечения информационной безопасности. В тоже время комплексный подход, используемый в современных концепциях информационной безопасности, основывается на практическом опыте компаний, специализирующихся на предоставлении услуг по защите информации. . Однако только математическое моделирование корпоративной сети позволяет обеспечить эффективность и гарантированность функционирования систем защиты. Принципы построения СОБИ КС должны быть основаны на научных предпосылках, научно обоснованной математической модели корпоративной сети, раскрывающей внутренние принципы функционирования корпораций. Только тогда, на основе математического моделирования можно будет построить обоснованную, с гарантиями по безопасности концепцию информационной безопасности корпорации. Актуальность данного раздела также в том, что модели эффективности и надежности функционирования корпоративных сетей разработаны сравнительно давно и детально изучены, а адекватные модели безопасности пока только разрабатываются.

Во втором разделе рассматриваются проблемы безопасности современных корпоративных сетей и формулируются научно-технические принципы построения СОБИ КС с учетом приведенной математической модели и современных тенденций развития сетевых информационных технологий. Выделяются особенности и

классификационные признаки корпоративных сетей. Приводятся структуры управления эффективностью и безопасностью корпоративной сети.

В третьем разделе систематизируются подходы к анализу защищенности корпоративных систем. Рассмотрены нормативная база, методики и средства для проведения подобного анализа.

Четвертая глава посвящена обзору современных технологий обеспечения защиты корпоративных сетей. Описываются наиболее популярные сегодня технологии межсетевых экранов, виртуальных частных сетей, систем обнаружения атак.

В пятой главе приведен подробный анализ возможных угроз со стороны внутренних злоумышленников, на долю которых согласно многочисленным исследованиям приходится до 80% всех нарушений в корпоративных сетях. Рассмотрена модель внутреннего нарушителя на основе рекомендаций Руководящих документов Гостехкомиссии России. На основе модели типовой корпоративной сети подробно изучены методы воздействий внутренних нарушителей на ресурсы корпоративных сетей. Пояснены методы защиты от каждой из рассмотренных угроз, а также предложены общие рекомендации по усилению защиты корпоративных сетей от внутренних нарушителей.

ГЛАВА 1. Элементы корпоративной модели информации

Введение

При построении сложных корпоративных систем защиты информации встает вопрос об оценке и учете *ценности* циркулирующих информационных потоков. В современной теории информации понятие ценности информации, как и само понятие информации, не определено строго и формально, что затрудняет определение уровней необходимых и достаточных механизмов защиты.

Действительно, для достижения наибольшей эффективности средства защиты должны адекватно защищать информацию, в соответствии с ее ценностью в корпорации. Недостаточная изученность вопросов количественной оценки ценности информации в современной науке не дает возможности оценки и обоснования необходимых затрат на построение систем защиты информационных и телекоммуникационных систем, обоснованных моментах их приложения и составе защитных функций. Одновременно, такая ситуация приводит к растущим затратам на компенсацию действия угроз безопасности информации ТКС и ИТ.

При рассмотрении вопросов построения сложных информационных систем получил распространение подход, основанный на эволюционно-генетической аналогии. Суть данного подхода в том, что функции защиты информационных систем во многом аналогичны работе иммунных систем биологических организмов. Таким образом, можно изучив природные методы защиты, перенести их по аналогии в информационные технологии. Поэтому в дальнейшем будут использоваться такие биологические термины, как, например, популяция, индивидуумы.

Понятие корпорации, ресурсов, системы

В технических средствах сообщение, используемое для обмена между двумя и более субъектами, состоит из последовательности дискретных символов, каждый из которых выбран из некоторого конечного множества. Размерность этого множества должна определяться размерностью популяции и, соответственно, возможностью создания разнообразных объединений по связи из членов

популяции. В дальнейшем под термином «корпорация» здесь будет пониматься именно такое объединение субъектов. **Корпорация – это объединение членов популяции, которые образуют связи по обмену информацией, понятной и согласованной внутри корпорации и защищенной («секретной» по Шеннону) от других членов популяции, на период времени жизни корпорации, длительность которой может отличаться от длительности жизни популяции и отдельных ее членов.**

Каждая популяция развивается внутри какой-либо системы, представленной различными объектами окружения индивидуумов популяции. Эти объекты мы назовем **системными ресурсами**. Для существования и развития каждому индивидууму необходимы ресурсы, которые являются конечными. Так как популяция растет, то в какой-то момент времени интересы индивидуумов к части ресурсов начинают пересекаться, в этот момент и появляется **конкуренция**.

Рассмотрим популяцию в ее наипростейшем виде. Имеется набор индивидуумов, каждый из которых контролирует какую-то часть ресурсов системы. Рассматриваемая популяция не содержит объединений, и, следовательно, все индивидуумы контролируют одинаковую часть системных ресурсов. На рис. 1 представлена схема популяции, в которой под кругом понимается индивидуум, под прямоугольником – часть контролируемых ресурсов.

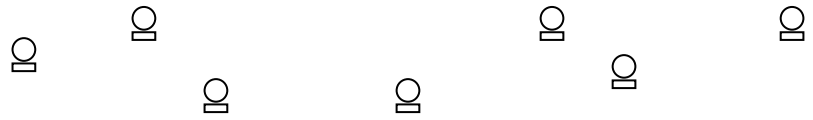

Рис 1.

На первоначальном этапе нет борьбы за распределение системных ресурсов между индивидуумами, так как отсутствует их фактическое взаимодействие в виду малого объема популяции. С ростом популяции индивидуумы начинают пытаться овладеть одной и той же частью системных ресурсов, то есть появляется взаимодействие. Для взаимодействия между индивидуумами необходим некий инструмент. Таким инструментом, являются **информация** и **язык**. Так как все индивидуумы обладают примерно одинаковыми начальными условиями, то появляется необходимость в создании групп индивидуумов, которые будут обладать большими системными ресурсами, чем одиночные индивидуумы, и, следовательно, смогут больше улучшить свое существование и ускорить развитие. Рост и

развитие корпораций определяется и ограничивается пересечением целей 3-х уровней: популяционного, корпоративного, субъектового.

При наличии информации, как инструмента борьбы за системные ресурсы, возникают объединения, то есть группы индивидуумов, контролирующих общую часть системных ресурсов. **Здесь информация выступает в роли характеристики системных ресурсов**. При помощи информации индивидуум в объединении контролирует часть системных ресурсов объединения, которая заведомо больше чем часть ресурсов, которые контролирует отдельный индивидуум. На рис 2. представлена схема популяции, в которой образовалось объединение.

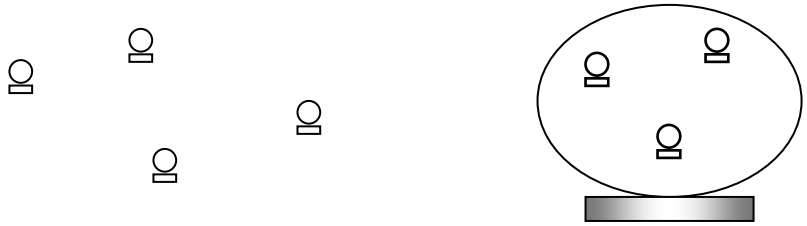

Рис 2.

После того, как в популяции образовались несколько объединений, необходим новый элемент для борьбы за ресурсы, которые или еще не распределены по объединениям, или за ресурсы самих объединений, причем между индивидуумами этих объединений. В этот момент и появляется язык, который способствует распределению информации между индивидуумами. Появление языка влечет за собой появление корпораций, в которых индивидуумы объединены для получения большего количества ресурсов и существуют связи для обмена информацией, то есть происходит как само накопление информации, так и ее распределение. Пример возникновения корпорации на рис 3.

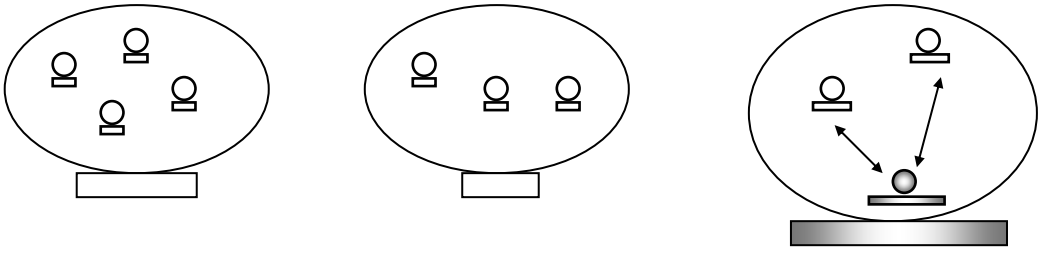

Рис 3

В корпорации каждый индивидуум при помощи языка устанавливает различные отношения с другими индивидуумами. В результате таких отношений возникает распределение информации внутри корпорации. Внешне же деятельность корпорации направлена на накопление корпоративных ресурсов и их сохранение. Так как информация это инструмент для накопления ресурсов, то возникает необходимость в ее защите. Потеря информации, которой располагают индивидуумы, т.е. индивидуальной информации, не может привести к большим потерям корпоративных ресурсов. Однако, при потере контроле над связями информационного обмена, корпорация может понести значительные убытки ресурсов. В этом случае теряются большие объемы информации, возможны замены истинной информации на ложную информацию, что в конечном итоге приводит к частичному контролю корпоративной деятельности.

Языковые связи и шифрование

Рассмотрим простейший пример взаимодействия внутри корпорации из трех индивидуумов. В такой корпорации не будем рассматривать ситуации с языковыми связями между всеми парами индивидуумов, так как это вырожденная ситуация и не дает преимущества никому из корпорации. Вариант языковой связи между двумя индивидуумами показан на рис 4.

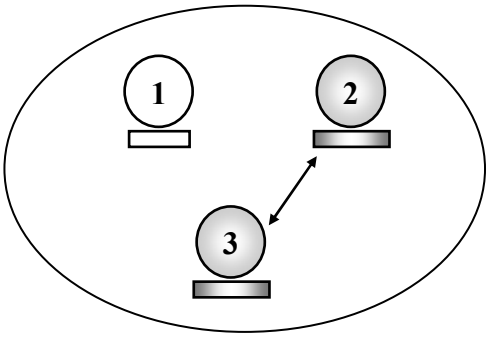

Рис 4.

Третий индивидуум устанавливает языковую связь со вторым. Этот обмен информацией направлен на увеличение объема контролируемых ресурсов, что происходит из-за получения новой информации. Здесь появляется понятие **ценности информации, это величина корпоративной информации, которую теоретически можно**

использовать, относительно всей информации, располагаемой корпорацией. В данной ситуации ценность информации первого индивидуума ноль, поскольку он не участвует в языковых связях, а второго и третьего – одна вторая, та как они образовывают корпорацию, состоящую из двух индивидуумов, внутри объединения.

На самом деле, пара индивидуумов, устанавливая связь, обменивается языковыми элементами, поочередные последовательности которых, приводят к перераспределению информации.

Индивидуумы внутри корпорации и в популяции в целом разрабатывают некоторый набор языков. Эти языки используются очень долгое время по сравнению со временами жизни корпораций и индивидуумов. Более того, языки развиваются вместе с корпорациями, что тоже

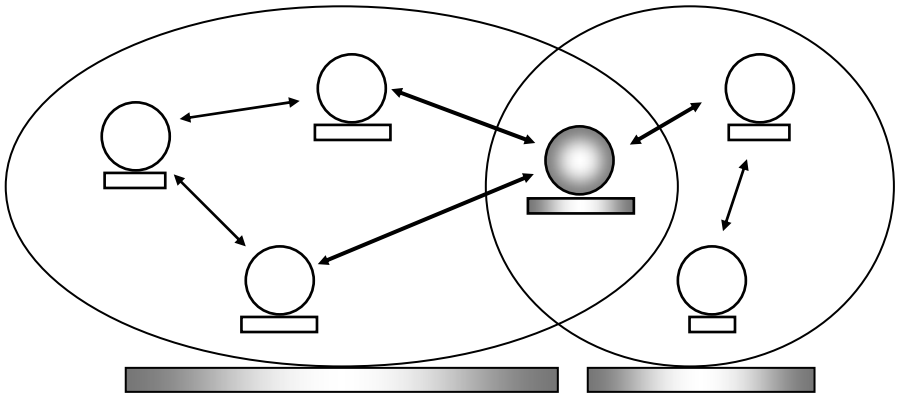

Рис 5.

составляет длительное время. Ясно, что одной из основных целей индивидуумов является размножение. Если бы после уничтожения (смерти) индивидуумов язык исчезал, то корпорации пришлось бы развиваться заново, поэтому языки передаются по наследству.

В разное или одно и то же время индивидуумы входят в состав разных корпораций. Поэтому через некоторое время одни и те же языки могут использоваться в разных связях и даже разных корпорациях. Такая ситуация описана на рис 5.

Проблема состоит в том, что информация, передаваемая через языковые связи, является конфиденциальной, иначе другие индивидуумы и корпорации имеют возможность прогнозировать ход борьбы за системные ресурсы.

Таким образом, возникает следующая ситуация: нельзя сменить язык в течение времени существования индивидуумов, использующих его в конкретном случае для обмена конфиденциальной информацией.

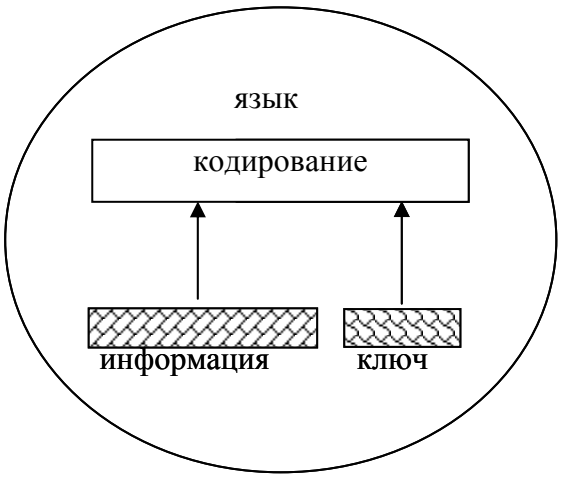

Рис 6.

Решение такой проблемы существует - это шифрование. В общем случае **шифрование представляет собой изменение выражения языка**, несущего некоторую часть передаваемой информации, при помощи некого механизма, который мы назовем **кодированием**, и **ключа**. Причем при отсутствии ключа и наличии кодирования из полученного (измененного) языкового выражения нельзя получить исходное выражение. Такой процесс передачи информации при помощи языка и шифрования представлен на рис 6.

То есть сам язык применяется только для организации связи, а выражения, которые передаются, не несут в явном виде информацию, представленную при помощи этого языка. Поэтому можно сказать, что фактически для организации связи используется известный язык и некая информация-ключ. Для передачи информации используется «новый» язык.

Таким образом, для конфиденциальной передачи информации индивидуумам одной корпорации, использующей эту информацию, достаточно знать язык, который очень тяжело перестроить, и ключ, который легко заменить. Время, необходимое для получения нового кодирования, сопоставимо со временем существования субъектов, что много меньше времени создания нового языка.

В дальнейшем корпорация развивается с использованием защищенного обмена. Время жизни индивидуума много меньше времени жизни корпорации. Но теперь, при наличии разработанного языка, индивидуум может все свое время существования потратить на улучшение своего состояния и развитие, учитывая интересы корпорации. Используя шифрование, он может не заботиться о технике передачи информации, а полностью посвятить себя ее распространению и получению. Конечно, какая-то малая часть индивидуумов должна заниматься вопросами шифрования, но эта часть незначительна по сравнению с объемом корпорации. Если бы пришлось разрабатывать

новые языки для обеспечения сохранности информации, то большая часть ресурсов корпорации тратилась бы на это, что значительно замедлило бы ее развитие. В случае использования шифрования, язык, кодирование и ключи передаются по наследству.

Защищенное распределение ключей

Следующим этапом в развитии корпорации с точки зрения защищенности обмена информацией является распределение ключей. Само распределение ключей появляется в тот момент, когда размеры и численность корпорации становятся достаточно большими. Кроме того, в корпорациях начинают появляться более мелкие корпорации, которые, могут пересекаться.

Сами по себе ключи становятся частью корпоративной и индивидуальной информации, поскольку также предназначены для обеспечения конкурентоспособности при захвате системных ресурсов. Распространенность языков и образование корпораций внутри корпораций приводит к тому, что ключи становятся неотъемлемой частью межкорпоративной конкуренции. В завершении всего корпорации начинают объединяться в новые корпорации, что опять-таки обусловлено тенденцией к захвату системных ресурсов.

В это время и возникает распределение ключей, создание которого повторяет развитие языка. То есть, можно сказать, что распределение ключей предоставляет корпорациям новые возможности для конкуренции. Если язык развивался на уровне индивидуумов, объединяющихся в корпорации, то распределение ключей сугубо корпоративное явление. Сравнительный процесс образования языка и распределения ключей показан на рис 7.

Распределение ключей необходимо для организации защищенных связей внутри и между разными большими корпорациями, также оно дает возможность индивидуумам устанавливать защищенные языковые связи на больших расстояниях, что приводит к появлению корпораций внутри других корпораций и способствует улучшению конкурентоспособности, как индивидуумов, так и корпораций в целом.

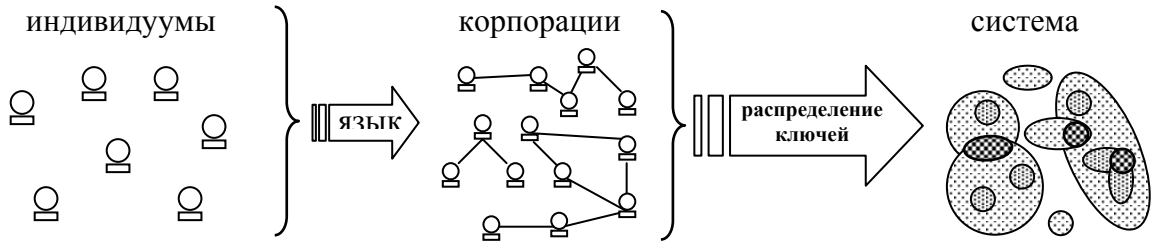

Рис 7.

В результате появляется полноценная система, в которой существуют все механизмы для борьбы за ресурсы. Такое количество инструментов значительно способствует развитию и увеличению корпоративной системы, что и является ее основной задачей.

Но для обеспечения защищенности корпораций необходимо устранить слабый момент в построении системы – защищенность распределения ключей.

Естественно, что развитие корпорации приводит к ее большим численным и территориальным размерам. Наступает время, когда субъекты не могут устанавливать связь, договорившись о ключе, в виду больших расстояний или иных условий, препятствующих этому. В это время вступает в силу механизм распределения ключей.

Возникает вопрос о защите этого механизма, ответ на который представлен в модели распределения ключей [1]. Модель распределения ключей должна обеспечивать сохранность конфиденциальности ключей и отзыв ключей в случае их компрометации.

Соотношение времен жизни популяции, корпорации и индивидуумов

Каждый индивидуум, естественно, имеет определенное время жизни, в течение которого он создает новые защищенные соединения, перераспределяет и приобретает информацию, участвует в создании новых индивидуумов. Корпорация же существует много больше времени, которое тратится на приобретение ресурсов, расширение и стабилизацию объема популяции.

Корпорация растет, пока в этом есть необходимость – для лучшей конкуренции необходимо большее количество субъектов. После чего численность популяции в корпорации стабилизируется, и конкуренция выражается в виде перераспределения и обработки информации. Уничтожение же корпорации происходит при потере необходимости в организации языковых связей между ее индивидуумами, или при исчерпании ресурсов.

Ценность корпоративной информации

Внутри корпораций субъекты образуют различные конфигурации, что приводит к неравноправию между ними. Это неравноправие выражается в ценности информации, которую они получают за счет образования конфигураций из языковых связей.

Для каждого индивидуума ценность информации будет заключаться в максимальном количестве информации, которую он может получить от всех языковых соединений относительно всей

информации в данной конфигурации. Для примера рассмотрим ситуацию, изображенную на рис 8.

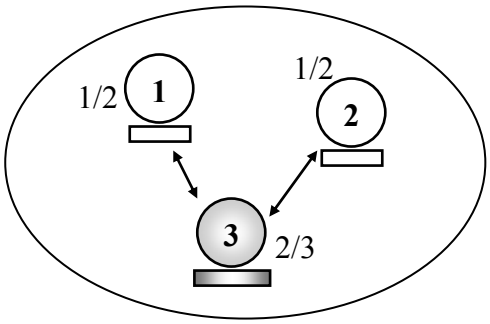

Рис 8.

В этой ситуации ценности информации первого и второго индивидуумов составляет одну вторую, так как они участвуют во взаимодействии только с один индивидуумом. Конфигурация же третьего индивидуума включает в себя два языковых соединения, и, следовательно, его максимальный выигрыш может составлять две третьих.

Понятие ценности информации позволяет оценить предпочтения индивидуумов при организации языковых связей. Но только желания индивидуумов недостаточны, необходимо также постоянно учитывать уровень защищенности, как конкретных связей, так и защищенность корпорации.

Аспекты практической защиты

Ценность данной модели должна подтверждаться ее практической пользой для построения защищенных корпоративных систем. Рассмотрим основные положения перехода от математической модели к практическим рекомендациям при построении систем защиты.

Одной из главных задач корпорации является сохранение ее коммерческих тайн, т.е. информации «которая обладает реальной или потенциальной экономической ценностью в силу того, что она не является общеизвестной и не может быть легко получена законным образом другими лицами, которые могли бы получить экономическую выгоду от ее разглашения или использования». Таким образом, эффективная работа организации невозможна без контроля за критическим ресурсами. Внутри рассматриваемой корпорации, в общем случае, можно выделить отдельные вложенные корпорации (например, отделы в организации). Какова должна быть их численность и архитектура этих корпораций, количество и характер взаимосвязей между ними определяется моделью безопасности корпоративной среды.

Если не уверен в безопасности, считай,
что опасность существует реально
Правила морского судоходства

ГЛАВА 2. Введение в безопасность корпоративных сетей

Проблемы безопасности современных корпоративных сетей

Новые информационные технологии активно внедряются во все сферы народного хозяйства. Появление локальных и глобальных сетей передачи данных предоставило пользователям компьютеров новые возможности оперативного обмена информацией. Если до недавнего времени подобные сети создавались только в специфических и узконаправленных целях (академические сети, сети военных ведомств и т.д.), то развитие Интернета и аналогичных систем привело к использованию глобальных сетей передачи данных в повседневной жизни практически каждого человека.

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий.

Актуальность и важность проблемы обеспечения информационной безопасности обусловлена следующими факторами:

- Современные уровни и темпы развития средств информационной безопасности значительно отстают от уровней и темпов развития информационных технологий.
- Высокие темпы роста парка персональных компьютеров, применяемых в разнообразных сферах человеческой деятельности.
  Согласно данным исследований компании Gartner Dataquest в настоящее время в мире более миллиарда персональных компьютеров. А следующий миллиард будет достигнут уже в 2008 году.
- Резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;
  Доступность средств вычислительной техники, и, прежде всего персональных ЭВМ, привела к распространению компьютерной грамотности в широких слоях населения. Это, в свою очередь, вызвало многочисленные попытки вмешательства в работу государственных и коммерческих систем, как со злым умыслом, так и из чисто «спортивного интереса». Многие из этих попыток

имели успех и нанесли значительный урон владельцам информации и вычислительных систем. По неофициальным данным до 70% всех противонарушений, совершаемых так называемыми хакерами, приходится на долю script-kiddies, в дословном переводе – дети, играющиеся со скриптами. Детьми их называют, потому что они не являются специалистами в компьютерных технологиях, но умеют пользоваться готовыми программными средствами, которые достают на хакерских сайтах в Интернете, для осуществления деструктивных действий.

- Значительное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;

  По оценкам специалистов в настоящее время около 70-90% интеллектуального капитала компании хранится в цифровом виде – текстовых файлах, таблицах, базах данных.
- Многочисленные уязвимости в программных и сетевых платформах;

  Стремительное развитие информационных технологий открыло новые возможности для бизнеса, однако привело и к появлению новых угроз. Современные программные продукты из-за конкуренции попадают в продажу с ошибками и недоработками. Разработчики, включая в свои изделия всевозможные функции, не успевают выполнить качественную отладку создаваемых программных систем. Ошибки и недоработки, оставшиеся в этих системах, приводят к случайным и преднамеренным нарушениям информационной безопасности. Например, причинами большинства случайных потерь информации являются отказы в работе программно-аппаратных средств, а большинство атак на компьютерные системы основаны на найденных ошибках и недоработках в программном обеспечении. Так, например, за первые полгода после выпуска серверной операционной системы компании Microsoft Windows Server 2003 было обнаружено 14 уязвимостей, 6 из которых являются критически важными. Несмотря на то, что со временем Microsoft разрабатывает пакеты обновления, устраняющие обнаруженные недоработки, пользователи уже успевают пострадать от нарушений информационной безопасности, случившихся по причине оставшихся ошибок. Такая же ситуация имеет место и с программными продуктами других фирм. Пока не будут решены эти многие другие проблемы, недостаточный уровень информационной безопасности будет серьезным тормозом в развитии информационных технологий.

- Бурное развитие глобальной сети Интернет, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире.

  Подобная глобализация позволяет злоумышленникам практически из любой точки земного шара, где есть Интернет, за тысячи километров, осуществлять нападение на корпоративную сеть.
- Современные методы накопления, обработки и передачи информации способствовали появлению угроз, связанных с возможностью *потери*, *искажения* и *раскрытия* данных, адресованных или принадлежащих конечным пользователям.

  Например, в настоящее время в банковской сфере свыше 90% всех преступлений связано с использованием автоматизированных систем обработки информации.

Под **угрозой** безопасности понимается возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику или пользователю, проявляющегося в опасности искажения, раскрытия или потери информации. Реализацию угрозы в дальнейшем будем называть атакой.

Реализация той или иной угрозы безопасности может преследовать следующие цели:

- нарушение **конфиденциальности** информации. Информация, хранимая и обрабатываемая в корпоративной сети, может иметь большую ценность для ее владельца. Ее использование другими лицами наносит значительный ущерб интересам владельца;
- нарушение **целостности** информации. Потеря целостности информации (полная или частичная, компрометация, дезинформация) - угроза близкая к ее раскрытию. Ценная информация может быть утрачена или обесценена путем ее несанкционированного удаления или модификации. Ущерб от таких действий может быть много больше, чем при нарушении конфиденциальности,
- нарушение (частичное или полное) работоспособности корпоративной сети (нарушение **доступности**). Вывод из строя или некорректное изменение режимов работы компонентов КС, их модификация или подмена могут привести к получению неверных результатов, отказу КС от потока информации или отказам при обслуживании. Отказ от потока информации означает непризнание одной из взаимодействующих сторон факта передачи или приема сообщений. Имея в виду, что такие сообщения могут содержать важные донесения, заказы,

финансовые согласования и т.п., ущерб в этом случае может быть весьма значительным.

Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий.

Корпоративная информационная система (сеть) - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы (из закона об Электронно-цифровой подписи).

Корпоративные сети (КС) относятся к распределенным компьютерным системам, осуществляющим автоматизированную обработку информации. Проблема обеспечения информационной безопасности является центральной для таких компьютерных систем. Обеспечение безопасности КС предполагает организацию противодействия любому несанкционированному вторжению в процесс функционирования КС, а также попыткам модификации, хищения, вывода из строя или разрушения ее компонентов, то есть защиту всех компонентов КС - аппаратных средств, программного обеспечения, данных и персонала.

Рассмотрим, как в настоящее время обстоит вопрос обеспечения ИБ на предприятии. Исследовательская компания Gartner Group выделяет 4 уровня зрелости компании с точки зрения обеспечения информационной безопасности (ИБ):

0 уровень:

ИБ в компании никто не занимается, руководство компании не осознает важности проблем ИБ;

Финансирование отсутствует;

ИБ реализуется штатными средствами операционных систем, СУБД и приложений (парольная защита, разграничение доступа к ресурсам и сервисам).

Наиболее типичным примером здесь является компания с небольшим штатом сотрудников, занимающаяся, например, куплей/продажей товаров. Все технические вопросы находятся в сфере ответственности сетевого администратора, которым часто является студент. Здесь главное, чтобы все работало.

1 уровень:

ИБ рассматривается руководством как чисто "техническая" проблема, отсутствует единая программа (концепция, политика) развития системы обеспечения информационной безопасности (СОИБ) компании;

Финансирование ведется в рамках общего ИТ-бюджета;

ИБ реализуется средствами нулевого уровня + средства резервного копирования, антивирусные средства, межсетевые экраны, средства организации VPN (традиционные средства защиты).

2 и 3 уровни:

ИБ рассматривается руководством как комплекс организационных и технических мероприятий, существует понимание важности ИБ для производственных процессов, есть утвержденная руководством программа развития СОИБ компании;

Финансирование ведется в рамках отдельного бюджета;

ИБ реализуется средствами первого уровня + средства усиленной аутентификации, средства анализа почтовых сообщений и web-контента, IDS (системы обнаружения вторжений), средства анализа защищенности, SSO (средства однократной аутентификации), PKI (инфраструктура открытых ключей) и организационные меры (внутренний и внешний аудит, анализ риска, политика информационной безопасности, положения, процедуры, регламенты и руководства).

3 уровень отличается от 2-го следующим:

ИБ является частью корпоративной культуры, назначен CISA (старший офицер по вопросам обеспечения ИБ);

Финансирование ведется в рамках отдельного бюджета, который согласно результатам исследований аналитической компании Datamonitor в большинстве случаев составляет не более 5% ИТ-бюджета;

ИБ реализуется средствами второго уровня + системы управления ИБ, CSIRT (группа реагирования на инциденты нарушения ИБ), SLA (соглашение об уровне сервиса).

Таким образом, серьезный подход к вопросам обеспечения ИБ появляется только на 2-м и 3-м уровнях. А на 1-м и частично 0-м уровне зрелости согласно данной классификации имеет место так называемый *«фрагментарный»* подход к обеспечению ИБ. *«Фрагментарный» подход* направлен на противодействие четко определенным угрозам в заданных условиях. В качестве примеров реализации такого подхода можно указать отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы и т.п.

Достоинство этого подхода заключается в высокой избирательности к конкретной угрозе. Существенным недостатком подхода является отсутствие единой защищенной среды обработки информации. Фрагментарные меры защиты информации обеспечивают защиту конкретных объектов КС только от конкретной угрозы. Даже небольшое видоизменение угрозы ведет к потере эффективности защиты.

Таких компаний по статистике Gartner – 85%.(0 – 30 %, 1 – 55%) по состоянию на 2001.

Более серьезные организации, соответствующие 2-му и 3-му уровням зрелости классификации Gartner, применяют *«комплексный»* подход к обеспечению ИБ. Этот же подход предлагают и крупные компании, профессионально занимающиеся защитой информации.

Комплексный подход основывается на решении комплекса частных задач по единой программе. Этот подход в настоящее время является основным для создания защищенной среды обработки информации в корпоративных системах, сводящей воедино разнородные меры противодействия угрозам. Сюда относятся правовые, морально-этические, организационные, программные и технические способы обеспечения информационной безопасности. Комплексный подход позволил объединить целый ряд автономных систем путем их интеграции в так называемые интегрированные системы безопасности.

Методы решения задач обеспечения безопасности очень тесно связаны с уровнем развития науки и техники и, особенно, с уровнем технологического обеспечения. А характерной тенденцией развития современных технологий является процесс тотальной интеграции. Этой тенденцией охвачены микроэлектроника и техника связи, сигналы и каналы, системы и сети. В качестве примеров можно привести сверхбольшие интегральные схемы, интегральные сети передачи данных, многофункциональные устройства связи и т. п.

Дальнейшим развитием комплексного подхода или его максимальной формой является **интегральный** подход, основанный на интеграции различных подсистем обеспечения безопасности, подсистем связи в единую **интегральную систему** с общими техническими средствами, каналами связи, программным обеспечением и базами данных. Интегральный подход направлен на достижение **интегральной безопасности.** Основной смысл понятия интегральной безопасности состоит в необходимости обеспечить такое состояние условий функционирования корпорации, при котором она надежно защищена от **всех возможных видов угроз** в ходе всего непрерывного производственного процесса. Понятие интегральной безопасности предполагает обязательную непрерывность процесса обеспечения безопасности как во времени, так и в пространстве (по всему технологическому циклу деятельности) с обязательным учетом всех возможных видов угроз (несанкционированный доступ, съем информации, терроризм, пожар, стихийные бедствия и т. д.).

В какой бы форме ни применялся комплексный или интегральный подход, он всегда направлен на решение ряда частных задач в их тесной взаимосвязи с использованием общих технических средств, каналов

связи, программного обеспечения и т. д. Например, применительно к информационной безопасности наиболее очевидными из них являются задачи ограничения доступа к информации, технического и криптографического закрытия информации, ограничения уровней паразитных излучений технических средств, охраны и тревожной сигнализации. Однако необходимо решение и других, не менее важных задач. Так, например, выведение из строя руководителей предприятия, членов их семей или ключевых работников должно поставить под сомнение само существование данного предприятия. Этому же могут способствовать стихийные бедствия, аварии, терроризм и т. п. Поэтому объективно обеспечить полную безопасность информации могут лишь интегральные системы безопасности, индифферентные к виду угроз безопасности и обеспечивающие требуемую защиту непрерывно, как во времени, так и в пространстве, в ходе всего процесса подготовки, обработки, передачи и хранения информации.

Комплексный подход к обеспечению информационной безопасности

К основным способам обеспечения информационной безопасности относят [2]:

- законодательные (правовые)
- морально-этические
- организационные (административные)
- технические
- программные

Законодательные меры защиты определяются законодательными актами страны, которыми регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Действительно, большинство людей не совершают противоправных действий вовсе не потому, что это технически сложно, а потому, что это осуждается и/или наказывается обществом, а также потому, что так поступать не принято.

Применительно к России сюда относятся:

- Конституция РФ от 23 февраля 1996 года
- Доктрина информационной безопасности РФ от 9 сентября 2000 г.
- Кодексы РФ
- Законы РФ

- Указы Президента РФ
- Постановления Правительства РФ
- Государственные стандарты в области защиты информации (ГОСТы)
- Руководящие документы (РД)

Конституция РФ

Статья 23 Конституции РФ гарантирует право граждан на личную и профессиональную тайны:

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

В части 4 статьи 29 перечислены действия, связанные с информацией, которые могут свободно осуществляться личностью: «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом». В этой же части статьи установлено ограничение на действия с информацией, составляющей государственную тайну.

Таким образом, статьи 23 и 29 Конституции РФ в современной интерпретации имеют отношение к конфиденциальной информации, передаваемой по компьютерным сетям.

Доктрина информационной безопасности России

Отметим, что доктрина по своему правовому статусу относится к организационно-распорядительным документам. То есть она носит информативный характер.

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере. В доктрине формулируются национальные интересы РФ в информационной сфере, виды и источники угроз ИБ РФ, задачи и методы обеспечения ИБ и т.д.

Кодексы РФ

Гражданский кодекс

В Гражданском кодексе Российской Федерации определены понятия **банковская, коммерческая и служебная тайна.** Согласно статье 139, информация составляет **служебную или коммерческую тайну** в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

Уголовный кодекс

В Уголовном кодексе РФ компьютерным правонарушениям посвящена глава 28:

- статья 272. Неправомерный доступ к компьютерной информации;
- статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Первая имеет дело с посягательствами на конфиденциальность, вторая - с вредоносным ПО, третья - с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ [3].

ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»

Статья 272 УК предусматривает ответственность за неправомерный доступ к компьютерной информации (информации на машинном носителе, в ЭВМ или сети ЭВМ), если это повлекло уничтожение, блокирование, модификацию либо копирование информации, а также нарушение работы вычислительных систем.

Данная статья защищает право владельца на неприкосновенность информации в системе. Владельцем информационной вычислительной системы может быть любое лицо, правомерно пользующееся услугами по обработке информации как собственник вычислительной системы (ЭВМ, сети ЭВМ) или как лицо, приобретшее право использования компьютера.

Неправомерным признается доступ к защищенной компьютерной информации лица, не обладающего правами на получение и работу с данной информацией, либо компьютерной системой.

Преступное деяние, ответственность за которое предусмотрено ст. 272 должно состоять в неправомерном доступе к охраняемой законом компьютерной информации, который всегда носит характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств позволяющих преодолеть установленные системы защиты; незаконного применения действующих паролей или маскировка под видом законного пользователя для проникновения в компьютер, хищения носителей информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации.

Важным является наличие причинной связи между несанкционированным доступом и наступлением предусмотренных статьей 272 последствий, поэтому простое временное совпадение момента сбоя в компьютерной системе, которое может быть вызвано неисправностями или программными ошибками и неправомерного доступа не влечет уголовной ответственности.

Неправомерный доступ к компьютерной информации должен осуществляться умышленно. Совершая это преступление, лицо сознает, что неправомерно вторгается в компьютерную систему, предвидит возможность или неизбежность наступления указанных в законе последствий, желает и сознательно допускает их наступление, либо относится к ним безразлично.

Мотивы и цели данного преступления могут быть любыми. Это и корыстный мотив, цель получить какую-либо информацию, желание причинить вред, желание проверить свои профессиональные способности. Следует отметить правильность действий законодателя, исключившего мотив и цель как необходимый признак указанного преступления, что позволяет применять ст. 272 УК к всевозможным компьютерным посягательствам.

Статья предусматривает наказание в виде штрафа от 200 минимальных размеров оплаты труда (МРОТ) до лишения свободы сроком до 5-ти лет при согрешении преступления группой лиц.

ст. 273 УК РФ "Создание, использование и распространение вредоносных программ для ЭВМ"

Статья предусматривает уголовную ответственность за создание программ для ЭВМ или их модификацию, заведомо приводящее к несанкционированному уничтожению, блокированию и модификации, либо копированию информации, нарушению работы информационных систем, а равно использование таких программ или машинных носителей с такими программами.

Статья защищает права владельца компьютерной системы на неприкосновенность находящейся в ней информации.

Под созданием вредоносных программам в смысле ст. 273 УК РФ понимаются программы, специально разработанные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций, для которых эти программы предназначены, определенные в документации на программу. Наиболее распространенными видами вредоносных программ являются широко известные компьютерные вирусы и логические бомбы.

Для привлечения к ответственности по 273 ст. необязательно наступление каких-либо отрицательных последствий для владельца информации, достаточен сам факт создания программ или внесение изменений в существующие программы, заведомо приводящих к негативным последствиям, перечисленным в статье.

Уголовная ответственность по этой статье возникает уже в результате создания программы, независимо от того использовалась эта программа или нет. По смыслу ст. 273 наличие исходных текстов вирусных программ уже является основанием для привлечения к ответственности. Следует учитывать, что в ряде случаев использование подобных программ не будет являться уголовно наказуемым. Это относится к деятельности организаций, осуществляющих разработку антивирусных программ и имеющих соответствующую лицензию.

Статья предусматривает наказание в виде лишения свободы на срок до 7 лет.

ст. 274 УК РФ "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети"

Статья 274 УК устанавливает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ним, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред.

Статья защищает интерес владельца вычислительной системы относительно ее правильной эксплуатации.

Данная уголовная норма, естественно, не содержит конкретных технических требований и отсылает к ведомственным инструкциям и правилам, определяющим порядок работы, которые должны устанавливаться специально управомоченным лицом и доводиться до пользователей.

Под охраняемой законом информацией понимается информация, для которой в специальных законах установлен специальный режим ее правовой защиты.

Между фактом нарушения и наступившим существенным вредом должна быть установлена причинная связь и полностью доказано, что наступившие последствия являются результатом именно нарушения правил эксплуатации.

Определение существенного вреда, предусмотренного в данной статье, - оценочный процесс, вред устанавливается судом в каждом конкретном случае, исходя из обстоятельств дела, однако очевидно, что существенный вред должен быть менее значительным, чем тяжкие последствия.

Преступник, нарушившее правило эксплуатации, - это лицо в силу должностных обязанностей имеющее доступ к компьютерной системе и обязанное соблюдать установленные для них технические правила.

Преступник должен совершать свое деяния умышленно, он сознает, что нарушает правила эксплуатации, предвидит возможность или неизбежность неправомерного воздействия на информацию и причинение существенного вреда, желает или сознательно допускает причинение такого вреда или относится к его наступлению безразлично. Что наиболее строго наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

В части второй статьи 274 предусматривается ответственность за неосторожные деяния. По ней должны квалифицироваться, например, действия специалиста по обслуживанию системы управления транспортом, установившего инфицированную программу без антивирусной проверки, повлекшее серьезную транспортную аварию.

Статья предусматривает наказание в виде лишения права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, и в самом крайнем случае - лишением свободы на срок до четырех лет.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Законы РФ

Закон РФ от 21 июля 1993 г. N 5485-1 "О государственной тайне" (с изменениями от 6 октября 1997 г.)

Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

В законе приведен перечень сведений составляющих государственную тайну. Это: 1) сведения в военной области (напр., о содержании стратегических и оперативных планов); 2) сведения в области экономики, науки и техники (например, сведения о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники); 3) сведения в области внешней политики и экономики; 4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

В законе изложены принципы отнесения сведений к государственной тайне и засекречивания этих сведений (статья 6), приведен перечень сведений, не подлежащих отнесению к государственной тайне и засекречиванию (статья 7). А в статье 8 устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: "особой важности" (ОВ), "совершенно секретно" (СС) и "секретно" (С).

ГОСТы

Из существующих ГОСТов в первую очередь представляет интерес «ГОСТ Р 50922-96. Защита информации. Основные термины и определения», в котором приведен список терминов из области защиты информации.

Например, защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

С 1 января 2004 года вступили в действие 3 новых ГОСТа, соответствующих международному стандарту Common Criteria.

ГОСТ Р ИСО/МЭК 15408-1

ГОСТ Р ИСО/МЭК 15408-2

ГОСТ Р ИСО/МЭК 15408-3

Руководящие документы (РД)

Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России) была создана в январе 1992 года Указом президента РФ для проведения единой технической политики и координации работ в области защиты информации. РД создаются Гостехкомиссией и устанавливают различные показатели, классы, нормативы защищенности средств вычислительной техники (СВТ) и автоматизированных систем (АС).

Основные руководящие и нормативные документы, созданные данной организацией можно посмотреть на официальном сайте Гостехкомиссии России в Интернете по адресу http://www.gostexkom.ru

В заключении обзора нормативно-правовой базы хотелось бы отметить, что эффективность действующего законодательства пока невысока. Отечественным законодательством преступления в сфере информационных технологий относятся к преступлениям средней тяжести – максимальный срок лишения свободы 7 лет. В развитых зарубежных странах, в которых информационные технологии играют значительную роль, планка максимального срока за компьютерные правонарушения гораздо выше – до 20-ти лет (в США). Действительно, принятая в апреле 2003 года в США «Стратегия национальной безопасности киберпространства» признает критическую зависимость экономической инфраструктуры США от информационных технологий. Поэтому ответственность за компьютерные правонарушения там строже. Что касается эффективности действующего законодательства – по данным управления «К» МВД РФ за 2001 год по статье 274 УК РФ было возбуждено только 8(!) уголовных дел. Причем 4 дела были прекращены, и только 3 дела дошли до суда.

К **морально-этическим** мерам противодействиям относятся нормы поведения, которые традиционно сложились или складываются по мере распространения сетевых и информационных технологий. Эти нормы большей частью не являются обязательными, как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета и престижа человека. Данные нормы могут быть оформлены в некоторый свод правил и предписаний.

Так, например, морально-этические принципы врачебной деятельности получили название клятвы Гиппократа. Наиболее показательным примером таких норм является Кодекс профессионального

поведения членов Ассоциации пользователей ЭВМ США. А на кафедре Безопасные Информационные Технологии сложилась традиция – все первокурсники принимают клятву защитника информации. В данной клятве сформулированы принципы, которым должны следовать обучающиеся по данной специальности.

Организационные (административные) средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и эксплуатация).

Организационные меры предусматривают:

- Ограничение доступа в помещения, в которых происходит обработка конфиденциальной информации.
- Допуск к решению задач на компьютер по обработке секретной, конфиденциальной информации проверенных должностных лиц, определение порядка проведения работ на компьютере.
- Хранение магнитных носителей в тщательно закрытых прочных шкафах.
- Назначение одного или нескольких компьютеров для обработки ценной информации и дальнейшая работа только на этих компьютерах.
- Установка дисплея, клавиатуры и принтера таким образом, чтобы исключить просмотр посторонними лицами содержания обрабатываемой информации.
- Постоянное наблюдение за работой принтера и других устройств вывода на материальных носитель ценной информации.
- Уничтожение красящих лент или иных материалов, содержащих фрагменты ценной информации.
- Запрещение ведения переговоров о непосредственном содержании конфиденциальной информации лицам, занятым ее обработкой.

Организационно-технические меры предполагают:

- Ограничение доступа внутрь корпуса компьютера путем установления механических запорных устройств.
- Уничтожение всей информации на винчестере компьютера при ее отправке в ремонт с использованием средств низкоуровневого

форматирования.

- Организацию питания компьютера от отдельного источника питания или от общей (городской) электросети через стабилизатор напряжения (сетевой фильтр) или мотор-генератор.
- Использование для отображения информации жидкокристаллических или плазменных дисплеев, а для печати - струйных или лазерных принтеров.
- Размещение дисплея, системного блока, клавиатуры и принтера на расстоянии не менее 2,5-3,0 метров от устройств освещения, кондиционирования воздуха, связи (телефона), металлических труб, телевизионной и радиоаппаратуры, а также других компьютеров, не использующихся для обработки конфиденциальной информации.
- Отключение компьютера от локальной сети или сети удаленного доступа при обработке на нем конфиденциальной информации, кроме случая передачи этой информации по сети.
- Установка принтера и клавиатуры на мягкие прокладки с целью снижения утечки информации по акустическому каналу.
- Во время обработки ценной информации на компьютере рекомендуется включать устройства, создающие дополнительный шумовой фон (кондиционеры, вентиляторы), а также обрабатывать другую информацию на рядом стоящих компьютерах. Эти устройства должны быть расположены на расстоянии не менее 2,5-3,0 метров.
- Уничтожение информации непосредственно после ее использования.

Технические средства реализуются в виде механических, электрических, электромеханических и электронных устройств, предназначенных для препятствования на возможных путях проникновения и доступа потенциального нарушителя к компонентам защиты. Вся совокупность технических средств делится на **аппаратные и физические.**

Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в телекоммуникационную аппаратуру, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу.

Например, в системе защиты рабочей станции Secret Net реализована добавочная аппаратная поддержка для идентификации пользователей по специальному электронному ключу.

Физические средства реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

Компоненты, из которых состоят современные комплексы защиты территории охраняемых объектов, включают:

- Механическая система защиты
  Реальное физическое препятствие, характеризующиеся временем сопротивления и включающее в себя датчики оповещения.
- Система оповещения
  Повышение вероятности обнаружения нарушителя системой оповещения обязательно сопровождается увеличением числа ложных срабатываний. Таким образом, разработка систем оповещения связана, прежде всего, с поиском рационального компромисса относительно соотношения величин названых показателей. Дальнейшее совершенствование систем оповещения должно обеспечить, прежде всего, повышение вероятности обнаружения и снижения интенсивности ложных срабатываний путем использования нескольких систем оповещения различного принципа действия в одном комплексе.

- Системы опознавания

Одно из условий надежного функционирования – анализ поступающих сообщений о проникновении для точного определения их типа.

Самый распространенный способ – телевизионные установки дистанционного наблюдения. Вся контролируемая системой оповещения зона делится на участки, на каждом из которых устанавливается 1 камера. При срабатывании датчиков оповещения, изображение, передаваемое телекамерой, выводится на экран монитора на центральном посту. Фактические причины срабатывания системы устанавливаются при условии высокой оперативности дежурного охранника.

Телевизионные системы могут применяться и для контроля действий персонала внутри объектов.

- Оборонительные системы

Используются для предотвращения развития вторжения на охраняемую территорию – обычно это осветительные или звуковые установки.

- Центральный пост и персонал охраны

Работа всех технических установок постоянно контролируется и управляется с центрального поста охраны, к центральным устройствам комплексов защиты предъявляются особые требования.

На данный момент из систем безопасности наиболее динамично развиваются системы контроля доступа (СКД), которые обеспечивают безопасность персонала и посетителей, сохранность материальных ценностей и информации и круглосуточно держат ситуацию на фирме под контролем.

Механические замки остаются более приемлемыми для небольших предприятий, несмотря на появление новейших СКД. Существует масса разнообразных замков повышенной секретности, как внутренних, так и наружных, которые могут использоваться для установки в местах, требующих специальной защиты. Производители продолжают рассматривать механические замки повышенной секретности в качестве гибкого, эффективного и недорогого средства обеспечения потребностей в защите собственности и наращивают объем их выпуска. Поэтому наличие механического ключа все еще остается простейщим идентификационным признаком при контроле доступа.

Еше одна группа средств идентификации это – удостоверения с фотографией владельца и жетоны. Удостоверения выдаются служащим фирмы, а жетоны – посетителям. Удостоверения и жетоны могут применяться вместе со средствами контроля доступа по карточкам, тем самым превращаясь в машиночитаемые пропуска. Для усиления защиты карточки с фотографией могут дополняться устройствами считывания и набором персонального кода.

Считается, что карточки-жетоны целесообразно использовать для прохода в контролируемые области на крупных предприятиях.

Существует широкий набор электронных СКД, среди которых большее место занимает аппаратура с применением микропроцессоров и компьютеров. Одним из достоинством подобного рода средств защиты является возможность анализа ситуации и ведения отчета.

К разряду электронных систем контроля доступа относятся системы с цифровой клавиатурой (кнопочные), с карточками и с электронными ключами. Клавиатура совместно с электрозамком в системах повышенной защищенности дополнены системой считывания карточек.

В системах контроля доступа по карточкам ключом является специальным образом закодированная карта, которая выполняет функцию удостоверения личности служащего.

Программные средства представляют из себя программное обеспечение, специально предназначенное для выполнения функций защиты информации.

Программные средства и составляли основу механизмов защиты на первой фазе развития технологии обеспечения безопасности связи в каналах телекоммуникаций. При этом считалось, что основными средствами защиты являются программные. Первоначально программные механизмы защиты включались, как правило, в состав операционных систем управляющих ЭВМ или систем управления базами данных. Практика показала, что надежность подобных механизмов защиты является явно недостаточной. Особенно слабым звеном оказалась защита по паролю. Поэтому в дальнейшем механизмы защиты становились все более сложными, с привлечением других средств обеспечения безопасности.

К данному классу средств защиты относятся: антивирусные, криптографические средства, системы разграничения доступа, межсетевые экраны, системы обнаружения вторжений и т.п.

Основные принципы обеспечения информационной безопасности

Построение системы защиты должно основываться на следующих основных принципах [4]:

- Системность подхода.
- Комплексности решений.
- Разумная достаточность средств защиты.
- Разумная избыточность средств защиты.
- Гибкость управления и применения.
- Открытость алгоритмов и механизмов защиты.
- Простота применения защиты, средств и мер.
- Унификация средств защиты.

Системность подхода

Защита информации предполагает необходимость учета всех взаимосвязанных и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения информационной безопасности.

При создании системы защиты необходимо учитывать все слабые и наиболее уязвимые места системы обработки информации, а также характер возможных объектов и нарушения атак на систему со стороны нарушителя, пути проникновения в систему для НСД к информации.

Система защиты должна строиться с учетом не только всех известных каналов проникновения, но и с учетом возможности появления преимущественно новых путей реализации угроз безопасности.

Системный подход также предполагает непротиворечивость применяемых средств защиты.

Различают следующие виды системности:

Пространственная системность

Может практиковаться как увязка вопросов защиты информации

по вертикали:

государство(правительственные органы)

↓

министерство

↓

корпоративные гос. учреждения

↓

частные предприятия

↓

автоматизированные системы обработки данных,
вычислительные системы

по горизонтали

пространственная системность предполагает увязку вопросов ЗИ в локальных узлах и территориях распределения элементов АСОД.

Временная системность (принцип непрерывности функционирования системы защиты):

Защита информации это не разовые мероприятия, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла защиты системы. Разработка системы защиты должна начинаться с момента проектирования системы защиты, а ее адаптация и доработка должна осуществляться на протяжении всего времени функционирования системы.

В частности по времени суток система защиты должна функционировать круглосуточно. Действительно, большинству средств защиты для выполнения своих функций необходима поддержка (администрирование), в частности для назначения и смены паролей, назначения секретных ключей, реакции на факты НСД и т.д. Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа защищаемых систем и СЗИ (средств защиты информации). Такие. перерывы в работе СЗИ могут использоваться для внесения закладок, совершения НСД и т.д.

Организационная системность

Означает единство организации всех работ по ЗИ и управления к их осуществлению. Организационная системность предполагает создание в масштабах государства стройной системы органов, профессионально ориентированных на ЗИ.

Комплексность мер и средств защиты

В распоряжении специалистов находится широкий спектр мер, методов и средств защиты информационных систем. Комплексное их использование или комплексирование предполагает согласованное применение разнородных средств защиты при обеспечении информационной безопасности. Данный принцип предполагает учет всей совокупности возможных угроз при реализации систем защиты.

Принцип разумной достаточности

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Поэтому при проектировании системы безопасности имеет смысл вести речь о некотором ее приемлемом уровне. При этом необходимо понимать, что высокоэффективная система защиты дорого стоит, может существенно снижать производительность защищаемого объекта и создавать ощутимые неудобства для пользователя.

Важно правильно выбрать тот правильный уровень защиты, при котором затраты, риск взлома и размер возможного ущерба были бы приемлемы.

Принцип разумной избыточности

Особенностью функционирования системы защиты является то, что уровень защищенности непрерывно снижается в процессе функционирования системы. Это вызвано тем, что любая атака на

систему как успешная, так и нет, дает информацию злоумышленнику. Накопление информации приводит к успешной атаке.

Сказанное находится в противоречии с принципом разумной достаточности. Выход здесь в разумном компромиссе – на этапе разработки системы защиты в нее должна закладываться некая избыточность, которая бы позволила увеличить срок ее жизнеспособности.

Принцип гибкости управления и применения (принип адаптивности)

Как правило, система защиты проектируется в условиях большой неопределенности. Поэтому устанавливаемые средства защиты могут обеспечивать как чрезмерный, так и достаточный уровень защищенности. Поэтому должны быть реализованы принципы гибкости управления, обеспечивающие возможность настройки механизмов в процессе функционирования системы. Так, введение какого-либо нового узла в корпоративной сети или изменение действующих условий не должно снижать достигнутого уровня защищенности корпоративной сети в целом.

Принцип открытости алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности, структурной безопасности и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможность преодоления системы защиты (даже автору).

Принцип простого (прозрачного) применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Они должны обладать интуитивно понятным интерфейсом, автоматической и автоматизированной настройки. Система защита должна по возможности минимально мешать работе пользователей, поэтому она должна функционировать в «фоновом» режиме, была незаметной и ненавязчивой.

Принцип унификации средств защиты

Современные системы защиты отличаются высоким уровнем сложности, что требует высокой квалификации обслуживающего персонала.

С целью упрощения администрирования систем безопасности целесообразно стремиться к их унификации, по крайней мере, в пределах предприятия.

Например, многие фирмы-разработчики СЗИ стремятся к унификации журналов регистрации систем обнаружения атак, межсетевых экранов.

Концепция информационной безопасности

Введение

Концепция разработана на основе опыта проведения практических работ по инспектированию, анализу уязвимостей, сертификации и аттестации по требованиям безопасности большого числа корпоративных сетей передачи данных и автоматизированных систем, коммуникационных провайдеров (операторов связи), ряда Главных Управлений Центрального Банка России, коммерческих банков, Государственных структур и коммерческих предприятий.

Общие положения

Основная цель концепции - определение методов и средств защиты и обеспечения безопасности информации, отвечающих интересам, требованиям и законодательству Российской Федерации в современных условиях необходимости использования ресурсов глобальных сетей передачи данных общего пользования для построения корпоративных защищенных и безопасных сетей.

Концепция формулирует научно-технические принципы построения систем обеспечения безопасности информационных ресурсов корпоративных сетей (СОБИ КС) с учетом современных тенденций развития сетевых информационных технологий, развития видов сетевых протоколов, их взаимной инкапсуляции и совместного использования.

Методической базой концепции являются следующие нормативные документы Гостехкомиссии РФ:

- РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» Гостехкомиссии России, Москва, 1992г.;
- РД «Защита от несанкционированного доступа к информации. Термины и определения» Гостехкомиссии России, Москва, 1992 г.;
- РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации к информации. Показатели защищенности от несанкционированного доступа к

информации к информации» Гостехкомиссии России, Москва, 1992 г.;

- РД «Автоматизированные системы. Защита от несанкционированного доступа к информации к информации. Классификация автоматизированных систем и требования по защите информации» Гостехкомиссии России, Москва, 1992 г.

Основной современной тенденцией развития сетей связи является их **глобализация, усложнение и интеграция**.

Интеграция сетевых и коммуникационных технологий заключается в совместном использовании и интеграции разнообразных сетевых протоколов, во взаимном использовании коммуникационными провайдерами ресурсов и средств передачи данных и стыковке транспортных и сервисных услуг.

Усложнение сетевых технологий связано с разработкой новых функциональных протоколов связи и передачи информации, обеспечивающих более качественную, и надежную связь, увеличение объемов и скорости передаваемой информации.

Например, для повышения безопасности передачи информации был разработан протокол IPSEC, который входит в новую версию протокола IPv6.

Тенденция **глобализации** определяется необходимостью объединения и взаимного использования информационных ресурсов, расположенных в удаленных районах и странах.

Эти три основные тенденции развития сетевых информационных технологий приводят к четвертой и определяющей тенденции:

«Эффективное и гибкое управление безопасностью и защитой передаваемой и обрабатываемой информации средствами централизованно-распределенного управления».

Эффективная интеграция невозможна без взаимного доверия и гарантий по безопасности информации коммуникационных провайдеров. В противном случае, интеграция приводит к финансовым и моральным потерям одной из сторон и **организационному разрушению сети.**

Рост сложности коммуникационных технологий приводит к неограниченному росту угроз безопасности информации, что в условиях отсутствия квалифицированной и гарантированной СОБИ КС приводит к **функциональному разрушению сети.**

Глобализация предусматривает резкое увеличение числа взаимодействующих субъектов обмена информацией, что при отсутствии управляемой СЗИ БИ гарантирует обратный от желаемого

эффект - гарантии по несанкционированному доступу и превращению ценной для клиентов сети информации в бесполезно перекачиваемый информационный мусор.

Вывод:

Корпоративная сеть на основе ресурсов сети передачи данных общего пользования с гарантиями управления по безопасности информации - это основная и перспективная цель развития информационных технологий.

С учетом указанных тенденций приведенная **концепция** формулирует научно-технические принципы, методы и выбор средств реализации СОБИ КС построенных на ресурсах сетей передачи данных общего пользования.

Определение корпоративной сети. Особенности корпоративных сетей

Корпоративная сеть - взаимосвязанная совокупность сетей, служб передачи данных и телеслужб, предназначенная для предоставления единого защищенного сетевого пространства ограниченному рамками корпорации кругу пользователей.

Основными особенностями корпоративных сетей являются:

1. Использование того же инструментария, что и при работе с сетью передачи данных общего пользования.
2. Доступ к информации предоставляется только ограниченной группе клиентов во внутренней сети организации. Внутренняя сеть представляет из себя локальную сеть, отделенную от глобальных сетей межсетевыми экранами (МЭ).
3. Циркулирует информация трех типов: **официальная** (распространение которой официально санкционируется и поощряется на уровне организации), **проектная** или **групповая** (предназначена для использования отдельной группой сотрудников, как правило, подлежит защите) и **неофициальная** (личная папка или каталог на сервере, служащие хранилищем статей, заметок и идей, к которыми можно поделиться с другими сотрудниками предприятия в общих интересах для обмена замечаниями или каких-то других целей.
4. Наличие централизованной системы управления (**эффективностью функционирования, безопасностью, живучестью**) корпоративной сетью.

Для существующих корпоративных АС свойственно:

1. Использование корпорациями распределенной модели вычислений. Однако в последние 5-10 лет в нашей стране и за рубежом набирают популярность технологии тонкого клиента.
2. Неотделимость корпоративных приложений от функциональных подразделений корпорации, поскольку часть прикладного кода располагается на станции-клиенте.
3. Необходимость одновременного контроля нескольких локальных вычислительных сетей, необходимость обмена центральной консоли сообщениями с платформами администрирования.
4. Широкий спектр используемых способов представления, хранения и передачи информации.
5. Интеграция данных различного назначения, принадлежащих различным субъектам, в рамках единых баз данных. И, наоборот, размещение необходимых некоторым субъектам данных в удаленных узлах сети (пример, текстовые отчеты, хранимые на рабочих станциях).
6. Абстрагирование владельцев данных от физических структур и места размещения данных.
7. Участие в процессе автоматизированной обработки информации большого количества пользователей и персонала различных категорий. Непосредственный и одновременный доступ к ресурсам (в том числе и информационным) большого количества пользователей (субъектов доступа) различных категорий.
8. Высокая степень разнородности средств вычислительной техники и связи, а также программного обеспечения.
9. Отсутствие специальной программно-аппаратной поддержки средств защиты в функциональных технических средствах, используемых в системе.

Классификационные признаки корпоративных сетей

В соответствии с введенным определением корпоративной сети ее состав в общем случае образуют следующие функциональные элементы:

Рабочие места (абоненты) корпорации, которые могут быть:

- сосредоточенными, или располагаться в рамках одного здания;
- распределенными, или рассредоточенными на некоторой в общем случае неограниченно большой территории.

Информационные серверы корпорации, предназначенные для хранения и обработки информационных массивов (баз данных) различного функционального назначения. Они также могут быть *сосредоточенными* либо *распределенными* на большой территории корпорации.

Средства телекоммуникации, обеспечивающие взаимодействие между собою рабочих станций и их взаимодействие с информационным серверами. Средства телекоммуникации в рамках корпорации могут быть:

- *выделенными* (либо арендованными), являющимися принадлежностью корпорации;
- *общего назначения* (существующие вне корпорации сети связи, средства которых используются корпорацией). Это, как правило, средства существующих сетей общего пользования.

Телеслужбы. В рамках корпорации информационное воздействие может быть реализовано в рамках одной (телефония, телетекст, видеотекст, телефакс); либо нескольких служб (интеграция служб), что должно обеспечиваться соответствующими средствами телекоммуникации и абонентских окончаний.

Система управления эффективностью функционирования корпоративной сети. В зависимости от реализуемого набора служб в корпоративной сети должны использоваться свои средства управления сетью, в частности средства маршрутизации и коммутации; средства администрирования, реализуемые с целью эффективного использования сетевых ресурсов. По возможности управления элементами корпоративной сети можно выделить:

- *управляемые* в рамках корпорации функциональные элементы (это собственные, или дополнительно вводимые в рамках корпоративной сети средства);
- *не управляемые* в рамках корпорации функциональные элементы, (в частности, маршрутизаторы и коммутаторы), являющиеся принадлежностью используемых корпорацией подсетей общего назначения.

Система управления безопасностью функционирования корпоративной сети. В корпоративной сети должны быть реализованы необходимые сетевые службы безопасности, должны использоваться соответственно средства безопасности.

Система обеспечения надежности корпоративной сети. Должны быть предусмотрены средства обеспечения работоспособности всей сети, либо ее фрагментов при отказах элементов сети.

Система диагностики и контроля. В рамках корпоративной сети должны быть предусмотрены средства контроля работоспособности отдельных функциональных элементов, система сбора информации об отказах и сбоях и предоставления ее системам обеспечения живучести; управления эффективностью функционирования; управления безопасностью. Для корпоративной сети должны быть разработаны средства диагностики, реализуемые как в процессе функционирования сети, так и профилактически.

Система эксплуатации. Кроме перечисленных функциональных элементов, корпоративные сети связи должны иметь план (гипотезу) процесса развития, в большой мере определяющий закладываемые в нее функциональные возможности, в частности на уровне протоколов взаимодействия сетевых компонент и возможности их интеграции.

Обобщая введенные признаки корпоративных сетей, получим возможную их классификацию:

- по набору функциональных элементов, рис.9.;
- по иерархии управления, рис.10; здесь под локальной подсистемой понимается некоторая функциональная подсистема, классификация которых для системы управления безопасностью приведена на рис.11, и где сама функциональная подсистема приведена на рис.12.;
- по набору (типу и количеству) объединяемых в рамках корпоративной сети подсетей общего пользования;
- по набору (типу и количеству) реализуемых в рамках корпоративной сети телеслужб.

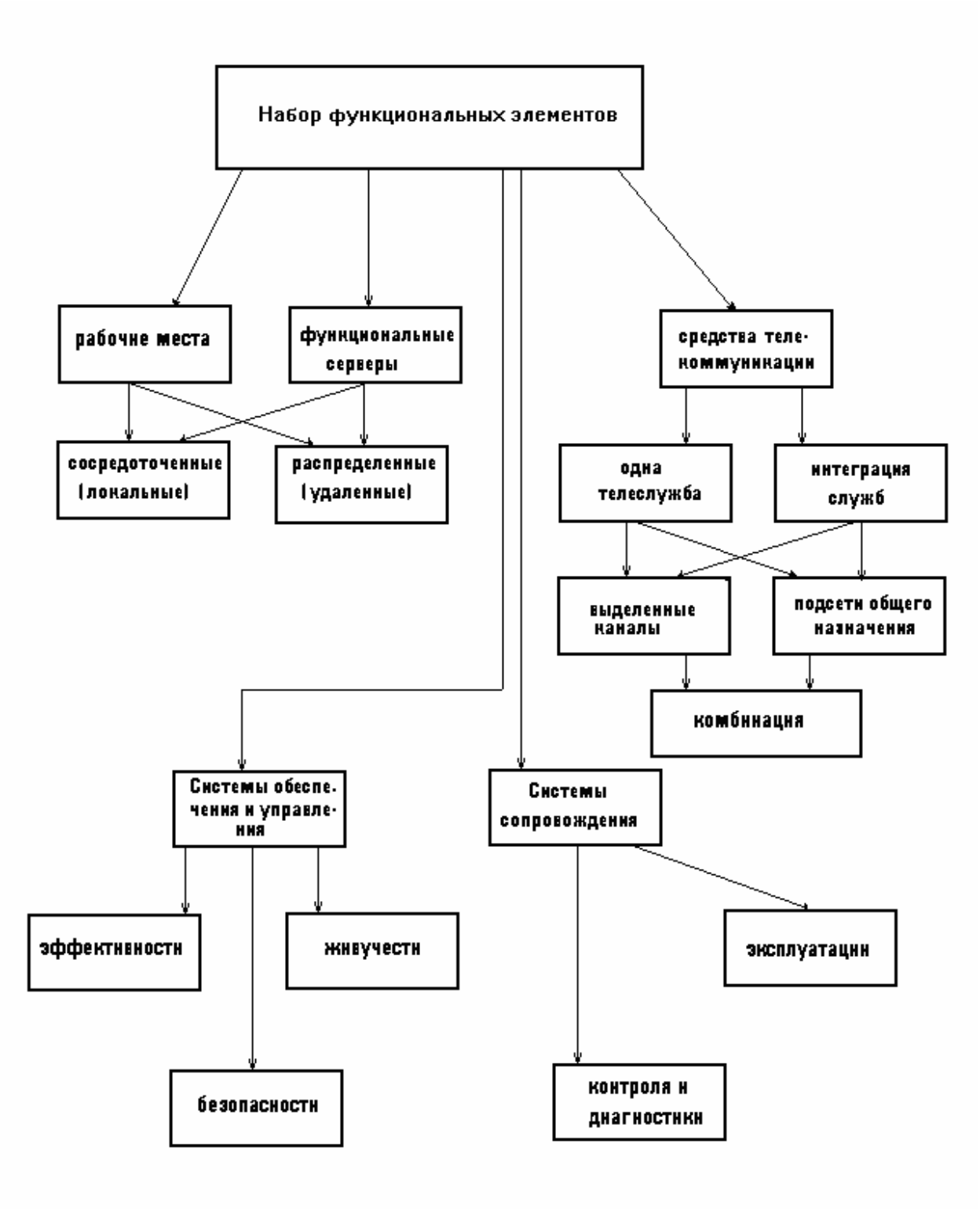

Рисунок 9. Функциональные компоненты корпоративных сетей

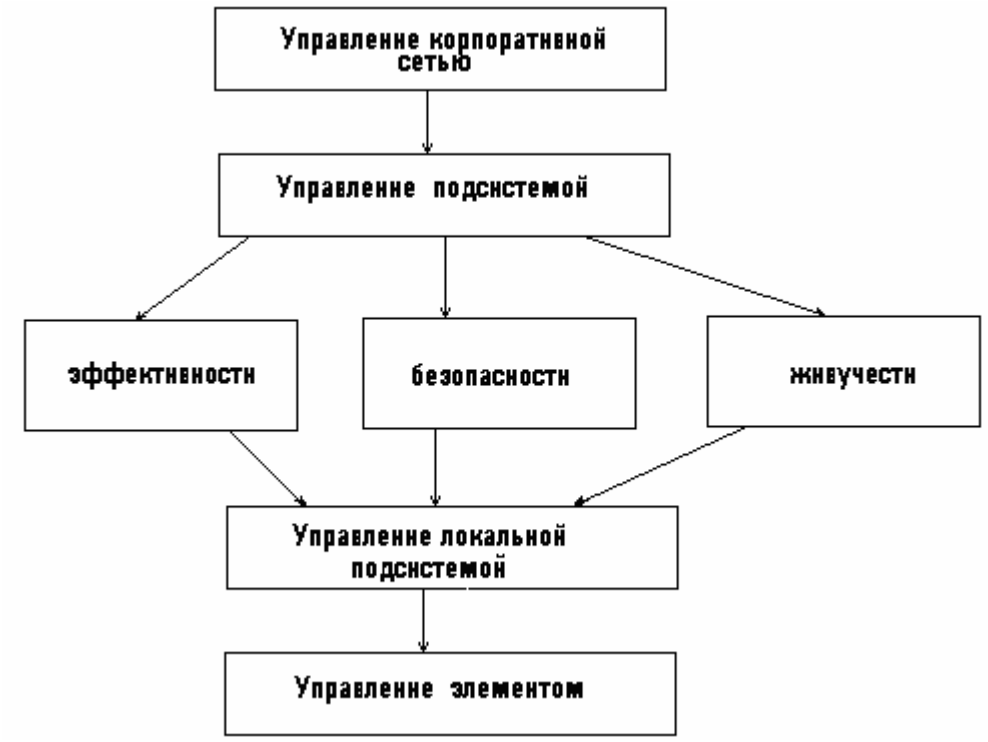

Рисунок 10. Классификация компонентов КС по иерархии управления

Рисунок 11. Классификация функциональных подсистем управления безопасностью

Рисунок 12. Элементы функциональной подсистемы

Обобщенная структура корпоративной сети, общие требования к администрированию сети

С учетом введенных классификационных признаков можно получить некоторую обобщенную структуру корпоративной сети, которая приведена на рис.13. Практически любая корпоративная сеть будет содержать фрагменты приведенной обобщенной структуры.

В рамках данной сети должна быть реализована вторичная сеть связи - система управления, представленная на рис.14.

Здесь также могут использоваться выделенные каналы (пунктир на рис.14 обозначает функциональную связь – физический канал проходит через средства маршрутизации, защиты и т.д., на рис.13).

В основе системы управления корпоративной сети должны лежать следующие принципы:

- совмещение администрирования отдельных функциональных подсистем (вопрос эффективности не может решаться вне рассмотрения вопроса живучести сети, а вопрос безопасности без учета эффективности и живучести (другими словами, при изменении уровня безопасности, например, изменяется и эффективность, что должно быть учтено);
- централизованное/распределенное администрирование, предполагающее, что основные задачи администрирования должны решаться из центра (основной фрагмент сети); вторичные

задачи (например, в рамках удаленных фрагментов) средствами управления отдельных подсистем;

- в рамках управляющей системы должны быть реализованы функции системы автоматического управления. С целью повышения оперативности реакции системы управления на особо важные события, в системе должна реализоваться автоматическая обработка особо важных воздействий;
- в рамках системы безопасности должен быть реализован адаптивного управления безопасностью адекватно изменению соответствующих событий (например, система обнаружения атак может блокировать локальный порт в случае атаки типа «отказ в обслуживании»).

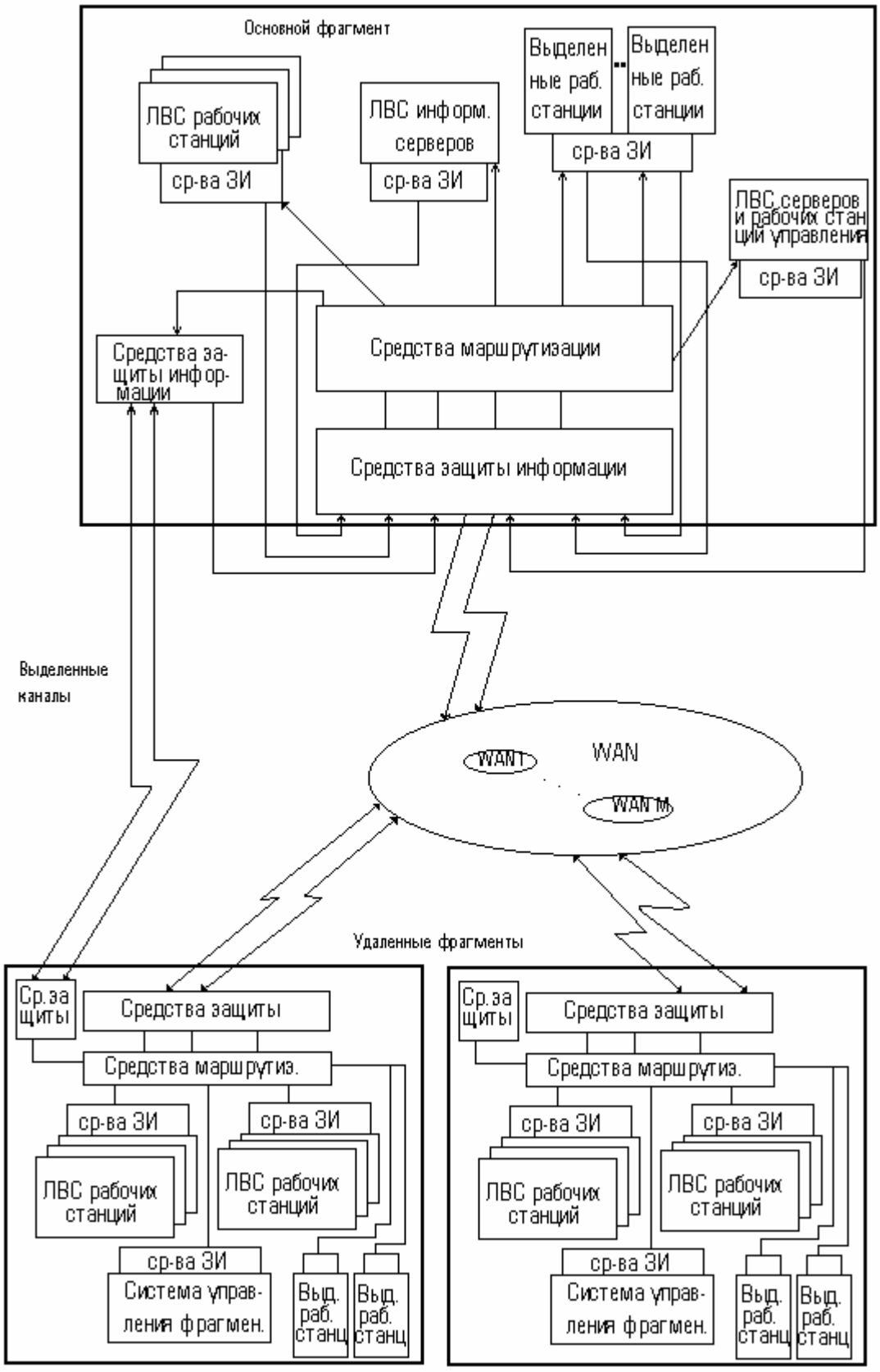

Рисунок 13. Обобщенная структура корпоративной сети

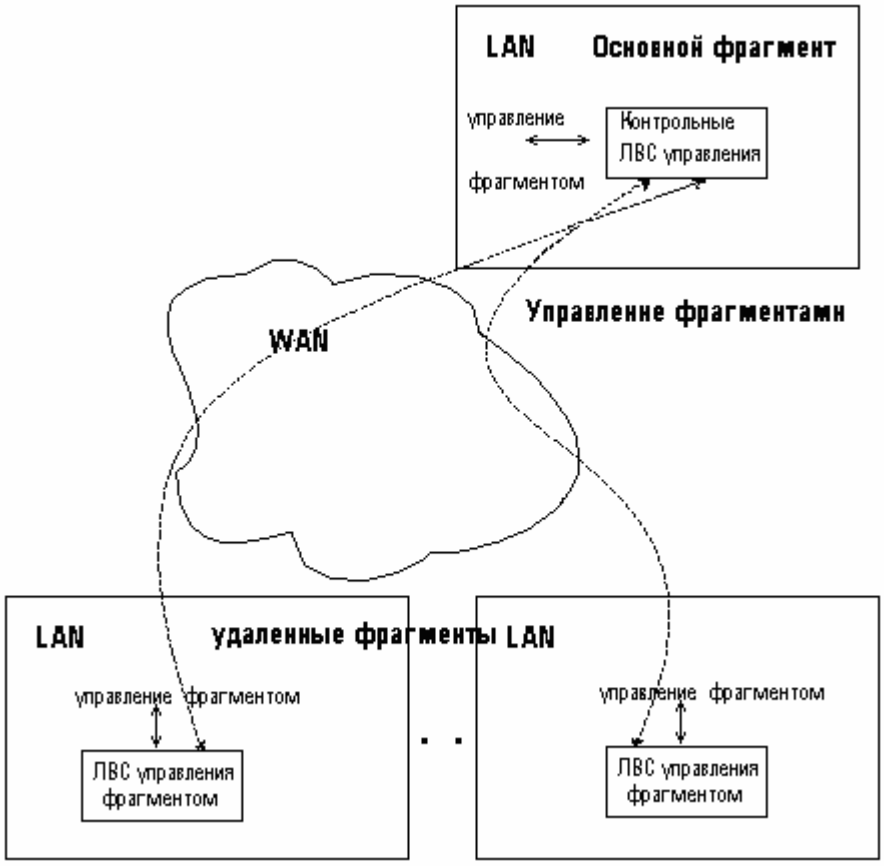

Рисунок 14. Система управления корпоративной сетью

- Для повышения эффективности и надежности системы управления необходимо предусмотреть экспертную систему – систему «подсказок» для выработки управляющих воздействий на различные события.

На рис.13 проиллюстрирован общий случай, отличающийся тем, что структуры основного и удаленного фрагментов совпадают (по функциям они различны - в основном фрагменте реализуется централизованное управление сетью связи). Как правило, данные фрагменты имеют различную сложность. При этом следует отметить, что упрощение структуры сети состоит в части уменьшения сложности удаленных фрагментов, с переносом соответствующих функций на элементы основного фрагмента, (соответственно с его усложнением), что, прежде всего, имеет место для следующих элементов:

- информационные серверы (с точки зрения обеспечения безопасности сети имеет смысл сконцентрировать все информационные серверы, обеспечивая для них необходимую защиту *организационными* и *техническими* мероприятиями);

- администрирование всеми функциональными подсистемами для корпоративных сетей, использующих ограниченное число дополнительных средств реализации функциональных подсистем (например, маршрутизаторов) может быть сконцентрировано в основном фрагменте;
- подключение к общедоступным сервисам (сеть Интернет) осуществляется с выделенных рабочих мест основного фрагмента (здесь используются соответствующие средства защиты, подключения к глобальным сетям в общем случае отличные от остальных).

С учетом сказанного, из рис.13. имеем упрощенную структуру корпоративной сети, структура которой приведена на рис.15.

Замечание. Именно структура корпоративной сети, приведенная на рис.15, может быть рекомендована как типовая для большинства мелких и средних корпораций (структура сети, приведенная на рис.13 предполагает реализацию сети для очень разветвленной инфраструктуры корпорации).

Итак, в данном разделе приведены два граничных варианта структур корпоративной сети, граничных в том смысле, что отличаются максимальной и минимальной сложностью структуры.

На практике большинство корпоративных сетей по сложности организации занимают некоторое промежуточное положение, соответственно в большей мере тяготея к одному из рассмотренных вариантов.

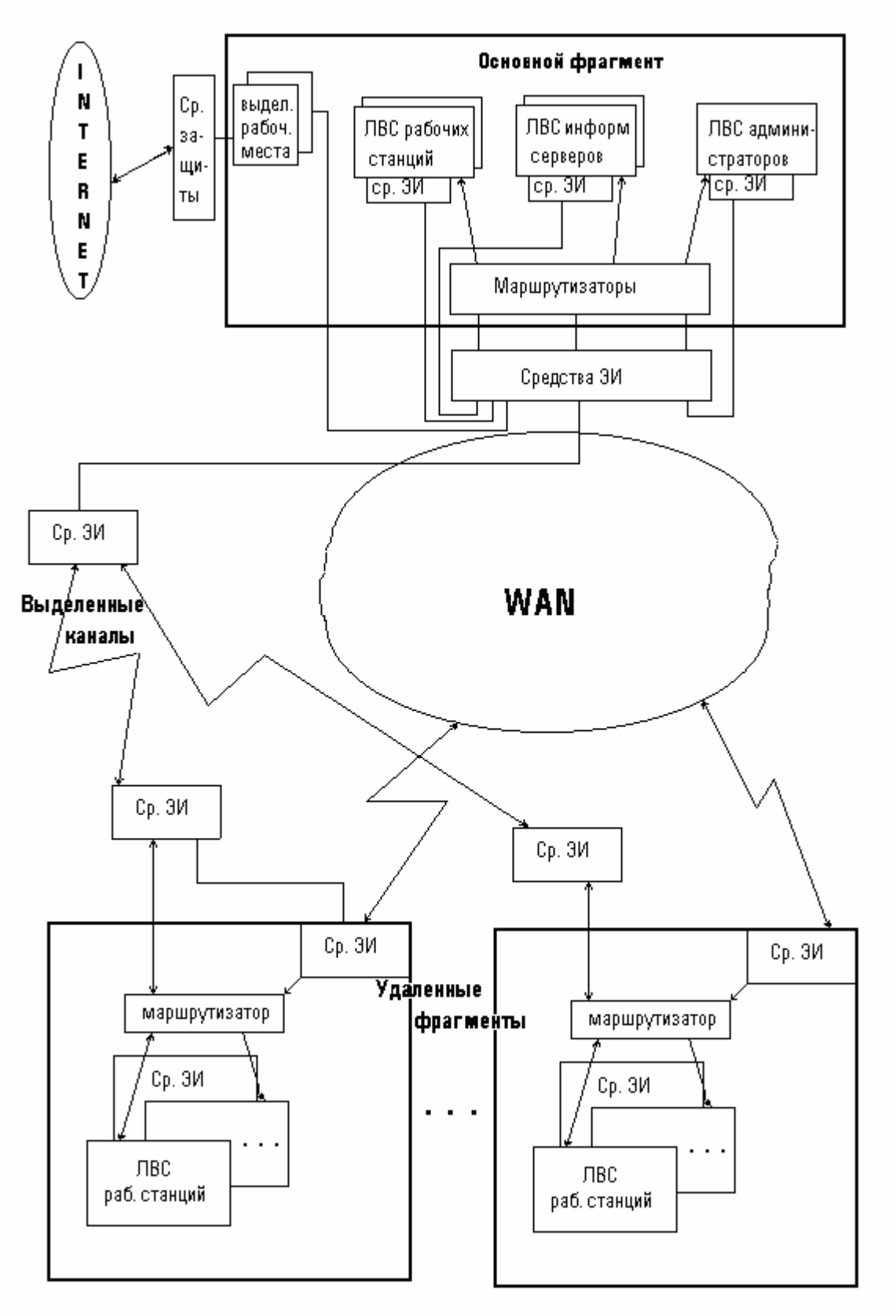

Рисунок 15. упрощенная структура корпоративной сети

Структура управления эффективностью функционирования сети. Основные требования

Рассмотрим структуру управления эффективностью функционирования сети в рамках приведенных структур сети и перечисленных ранее основных принципов администрирования.

В рамках корпоративной, как и в любой иной сети связи, должны быть реализованы все основные функции сетевых протоколов корпоративных сетей:

- маршрутизация;
- коммутация;
- управление потоками (обеспечение эффективности функционирования при высокой загрузке);
- контроль времени жизни пакета.

Также как в любой иной сети задачи управления эффективностью решаются в рамках вторичной (наложенной) сети связи.

Эффективное управление функционированием корпоративной сети может быть обеспечено только при динамической маршрутизации, где маршруты должны выбираться адаптивно к топологии и нагрузки в сети.

Замечание. Изменение маршрутов адаптивно к изменению топологии реализуется совместно с системой управления живучестью сети.

Иерархическая структура системы управления эффективностью приведена на рис.16, где маршрутизатор может рассматриваться в качестве узла коммутации корпоративной сети.

Замечание. WAN общего пользования закрыты для управления в рамках корпоративной сети (если только это не сети X.25, где при установлении соединения возможно согласование качества обслуживания, включая задание маршрутов), поэтому в общем случае фрагмент сети WAN следует рассматривать как виртуальный (не управляемый) канал.

Структура системы управления эффективностью корпоративной сети представлена на рис.17, потоки информации в системе управления проиллюстрированы на рис.18.

Идеология централизованного/распределенного управления эффективностью состоит в следующем:

- из единого центра реализуется управление узлами коммутации (маршрутизаторами, именно это позволяет строить эффективные корпоративные сети);

- локальные администраторы фрагментов управляют соответствующими ЛВС.

Отсюда получаем следующие требования к элементам управления:

- администратор корпоративной сети должен осуществлять сбор информации о состоянии сетевых компонент, в том числе и от удаленных фрагментов; должен обрабатывать эту информацию в соответствии с реализуемым алгоритмом управления, должен вырабатывать и выдавать к объектам управления соответствующие команды;
- маршрутизатор должен удалено управляться; осуществлять сбор обработки и передачу информации (в рамках системы сбора информации) о состоянии соответствующих компонент корпоративной сети;
- администраторы ЛВС должны обеспечивать сбор обработки и передачу необходимой информации о состоянии сетевых компонент ЛВС, управлять ЛВС в рамках прописанных полномочий.

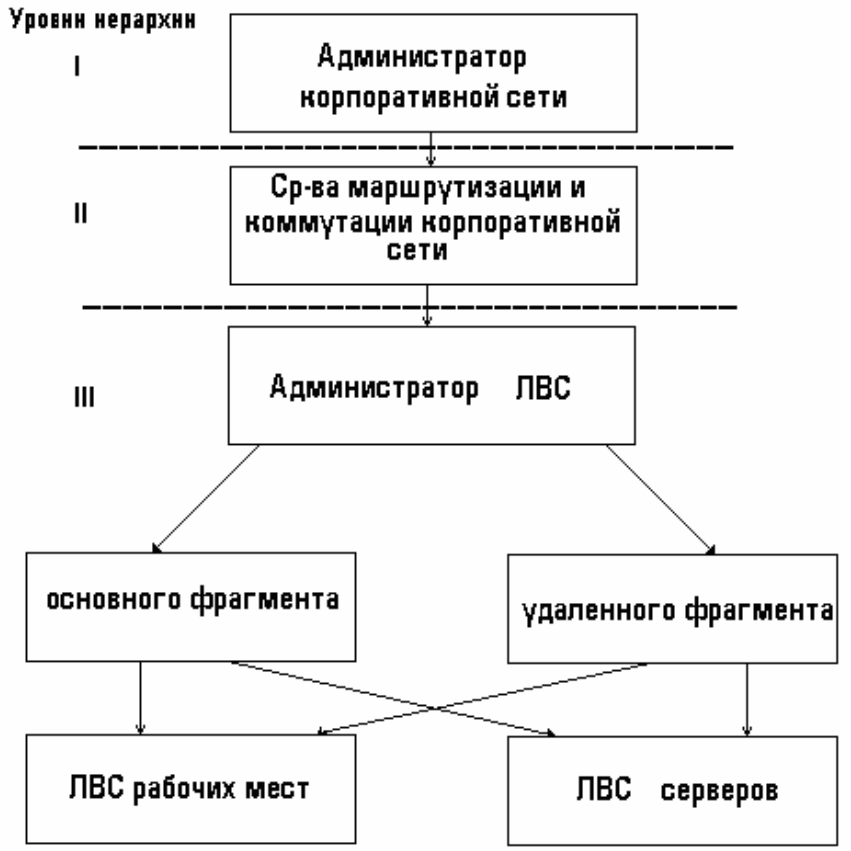

Рисунок 16. Иерархическая структура системы управления эффективностью

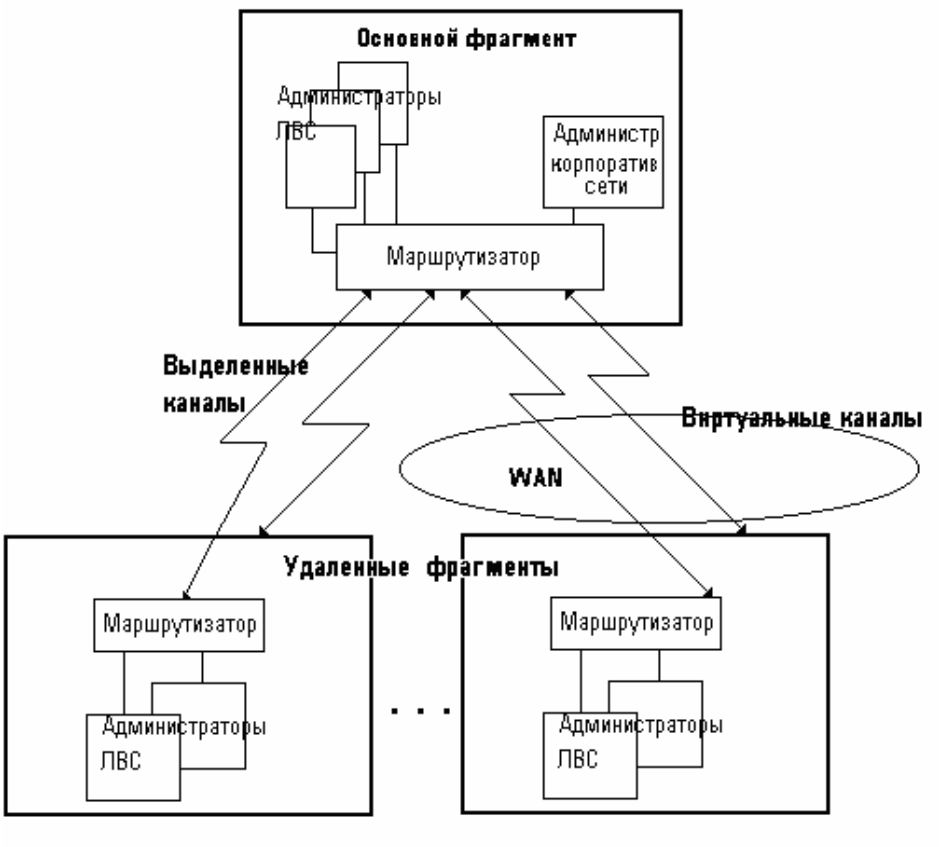

Рисунок 17. Обобщенная структура системы управления эффективностью.

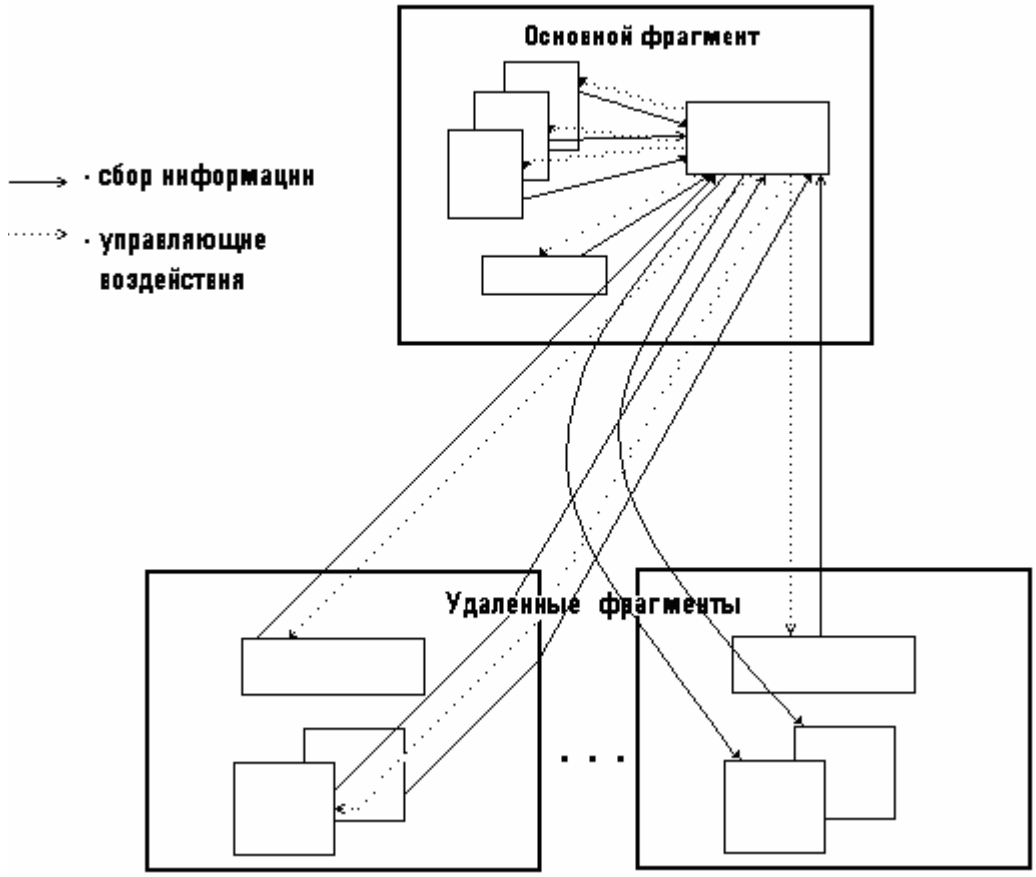

Рисунок 18. Потоки информации в системе управления.

Структура управления безопасностью сети. Основные требования

Система обеспечения безопасности информации должна иметь многоуровневую структуру и включать следующие уровни:

- уровень защиты автоматизированных рабочих мест (АРМ);
- уровень защиты локальных сетей и информационных серверов;
- уровень защиты корпоративной АС.

На **уровне защиты автоматизированных рабочих мест** должна осуществляться идентификация и аутентификация пользователей операционной системы. Должно осуществляться управление доступом: предоставление доступа субъектов к объектам в соответствии с матрицей доступа, выполнение регистрации и учета всех действий субъекта доступа в журналах регистрации. Должна быть обеспечена целостность программной среды, периодическое тестирование средств

защиты информации. Рекомендуется обеспечение защиты сертифицированными Гостехкомиссией России средствами защиты от несанкционированного доступа. Такие средства защиты должны обладать гибкими средствами настройки и возможностью удаленного администрирования.

Уровень защиты локальных сетей и сетевых серверов должен обеспечивать:

- идентификацию пользователей и установление подлинности доступа в систему, к компонентам;
- защиту аутентификационных данных;
- установление подлинности при доступе к серверам;
- пропуск аутентификационной информации от одного компонента до другого без переустановки подлинности доступа.

Механизмы защиты должны быть способны создавать, обслуживать (поддерживать) и защищать от модификации или неправомочного доступа или разрушения аутентификационную информацию и матрицу доступа к объектам.

Должна осуществляться регистрация следующих событий:

- использование идентификационных и аутентификационных механизмов;
- действия пользователей с критическими объектами;
- уничтожения объектов;
- действия, предпринятые операторами и администраторами системы и/или офицерами безопасности;
- другие случаи безопасности.

Параметры регистрации:

- дата и время события;
- пользователь;
- тип случая;
- успешная или неуспешная попытка

для идентификации/аутентификации дополнительно

- происхождение запроса (например, локальная или сетевая аутентификация);

для случаев уничтожения объектов и доставки информации в место адреса пользователя:

- название объекта.

Администратор системы должен быть способен выборочно контролировать действия любого пользователя или группы пользователей на основании индивидуальной идентичности.

Средства защиты информации должны иметь модульную структуру, каждый модуль должен поддерживать область памяти для собственного выполнения. Для каждого модуля СЗИ, каждого компонента СЗИ, разделенного в АС, должна обеспечиваться изоляция ресурсов, нуждающихся в защите так, чтобы они подчинялись контролю доступа и требованиям ревизии.

Периодическое тестирование правильности функционирования аппаратных средств, микропрограммных элементов СЗИ, программного обеспечения СЗИ.

При разделении СЗИ должна обеспечиваться способность сообщения административному персоналу об отказах, ошибках, попытках несанкционированного доступа, обнаруженных в разделенных компонентах СЗИ. Протоколы, осуществленные в пределах СЗИ, должны быть разработаны так, что должно обеспечиваться правильное функционирование СЗИ в случае отказов (сбоев) коммуникационной сети или ее индивидуальных компонентов.

Механизмы безопасности должны быть проверены и функционировать в соответствии с требованиями документации.

Уровень защиты корпоративной АС должен гарантировать:

1. Целостность передачи информации от ее источников до адресата:
- Аутентификацию;
- Целостность коммуникационного поля;
- Невозможность отказа партнеров по связи от факта передачи или приема сообщений.

2. Безотказность в предоставлении услуг
- Непрерывность функционирования;
- Устойчивость к атакам типа «отказ в обслуживании»;
- Защищенный протокол передачи данных.

3. Защиту от несанкционированного раскрытия информации:
- Сохранение конфиденциальности данных с помощью механизмов шифрования;
- Выбор маршрута передачи.

Средства защиты должны обеспечивать:

Конфиденциальность содержания (отправитель должен быть уверен, что никто не прочитает сообщения, кроме определенного получателя);

Целостность содержания (получатель должен быть уверен, что содержание сообщения не модифицировано);

Целостность последовательности сообщений (получатель должен быть уверен, что последовательность сообщений не изменена);

Аутентификацию источника сообщений (отправитель должен иметь возможность аутентифицироваться у получателя как источник сообщения, а также у любого устройства передачи сообщений, через который они проходят);

Доказательство доставки (отправитель может убедиться в том, что сообщение доставлено неискаженным нужному получателю);

Доказательство подачи (отправитель может убедиться в идентичности устройства передачи сообщения, на которое оно передано);

Безотказность источника (позволяет отправителю доказать получателю, что переданное сообщение принадлежит ему);

Безотказность поступления (позволяет отправителю сообщения получить от устройства передачи сообщения, на которое оно поступило, доказательство того, что сообщение поступило на это устройство для доставки определенному получателю);

Безотказность доставки (позволяет отправителю получить от получателя доказательство получения им сообщения);

Управление контролем доступа (позволяет двум компонентам системы обработки сообщений установить безопасное соединение);

Защиту от попыток расширения своих законных полномочий (на доступ, формирование, распределение и т.п.), а также изменения (без санкции на то) полномочий других пользователей;

Защиту от модификации программного обеспечения путем добавления новых функций.

Безопасность это процесс, а не результат.
Bruce Schneier

ГЛАВА 3. Анализ уровня защищенности корпоративной информационной системы

При создании информационной инфраструктуры корпоративной автоматизированной системы (АС) на базе современных компьютерных сетей неизбежно возникает вопрос о защищенности этой инфраструктуры от угроз безопасности информации. Насколько адекватны реализованные в АС механизмы безопасности существующим рискам? Можно ли доверять этой АС обработку (хранение, передачу) конфиденциальной информации? Имеются ли в текущей конфигурации АС ошибки, позволяющие потенциальным злоумышленникам обойти механизмы контроля доступа? Содержит ли установленное в АС программное обеспечение (ПО) уязвимости, которые могут быть использованы для взлома защиты? Как оценить уровень защищенности АС и как определить является ли он достаточным в данной среде функционирования? Какие контрмеры позволят реально повысить уровень защищенности АС? На какие критерии оценки защищенности следует ориентироваться и какие показатели защищенности использовать?

Такими вопросами рано или поздно задаются все специалисты ИТ-отделов, отделов защиты информации и других подразделений, отвечающих за эксплуатацию и сопровождение АС. Ответы на эти вопросы далеко неочевидны. Анализ защищенности АС от угроз безопасности информации — работа сложная. Умение оценивать и управлять рисками, знание типовых угроз и уязвимостей, критериев и подходов к анализу защищенности, владение методами анализа и специализированным инструментарием, знание различных программно-аппаратных платформ, используемых в современных компьютерных сетях — вот далеко не полный перечень профессиональных качеств, которыми должны обладать специалисты, проводящие работы по анализу защищенности АС.

Анализ защищенности является основным элементом таких взаимно пересекающихся видов работ как аттестация, аудит и обследование безопасности АС.

Понятие защищенности АС

Защищенность является одним из важнейших показателей эффективности функционирования АС, наряду с такими показателями как *надежность, отказоустойчивость, производительность* и т. п.

Под защищенностью АС будем понимать степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации [5]**.**

Под угрозами безопасности информации традиционно понимается возможность нарушения таких свойств информации, как конфиденциальность, целостность и доступность.

На практике всегда существует большое количество неподдающихся точной оценке возможных путей осуществления угроз безопасности в отношении ресурсов АС. В идеале каждый путь осуществления угрозы должен быть перекрыт соответствующим механизмом защиты. Данное условие является **первым фактором,** определяющим защищенность АС. **Вторым фактором** является прочность существующих механизмов защиты, характеризующаяся степенью сопротивляемости этих механизмов попыткам их обхода либо преодоления. **Третьим фактором** является величина ущерба, наносимого владельцу АС в случае успешного осуществления угроз безопасности.

На практике получение точных значений приведенных характеристик затруднено, т. к. понятия угрозы, ущерба и сопротивляемости механизма защиты трудноформализуемы. Например, оценку ущерба в результате НСД к информации политического и военного характера точно определить вообще невозможно, а определение вероятности осуществления угрозы не может базироваться на статистическом анализе. Оценка степени сопротивляемости механизмов защиты всегда является субъективной.

Нормативная база анализа защищенности

Наиболее значимыми нормативными документами в области информационной безопасности, определяющими критерии для оценки защищенности АС, и требования, предъявляемые к механизмам защиты, являются:

1. Общие критерии оценки безопасности ИТ (The Common Criteria for Information Technology Security Evaluation/ISO 15408).
2. Практические правила управления информационной безопасностью (Code of practice for Information Security Management/ISO 17799).

Кроме этого, в нашей стране первостепенное значение имеют Руководящие документы (РД) Гостехкомиссии России.

ISO15408: Common Criteria for Information Technology Security Evaluation

Наиболее полно критерии для оценки механизмов безопасности программно-технического уровня представлены в международном стандарте ISO 15408: Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий), принятом в 1999 году. В 2004 году в России был приняты три новых ГОСТа ГОСТ Р ИСО/МЭК 15408-1, ГОСТ Р ИСО/МЭК 15408-2, ГОСТ Р ИСО/МЭК 15408-3, являющиеся аутентичными переводами международного стандарта ISO 15408.

Общие критерии оценки безопасности информационных технологий (далее «Общие критерии») определяют функциональные требования безопасности (security functional requirements) и требования к адекватности реализации функций безопасности (security assurance requirements).

При проведении работ по анализу защищенности АС, а также средств вычислительной техники (СВТ) «Общие критерии» целесообразно использовать в качестве основных критериев, позволяющих оценить уровень защищенности АС (СВТ) с точки зрения полноты реализованных в ней функций безопасности и надежности реализации этих функций.

Хотя применимость «Общих критериев» ограничивается механизмами безопасности программно-технического уровня, в них содержится определенный набор требований к механизмам безопасности организационного уровня и требований по физической защите, которые непосредственно связаны с описываемыми функциями безопасности.

Первая часть «Общих критериев» содержит определение общих понятий, концепции, описание модели и методики проведения оценки безопасности ИТ. В ней вводится понятийный аппарат, и определяются принципы формализации предметной области.

Требования к функциональности средств защиты приводятся во **второй части** «Общих критериев» и могут быть непосредственно использованы при анализе защищенности для оценки полноты реализованных в АС (СВТ) функций безопасности.

• **Третья часть** «Общих критериев» содержит классы требований гарантий оценки.

Процедура аудита безопасности АС включает в себя проверку наличия перечисленных ключевых средств контроля, оценку полноты и

правильности их реализации, а также анализ их адекватности рискам, существующим в данной среде функционирования. Составной частью работ по аудиту безопасности АС также является анализ и управление рисками.

РД Гостехкомиссии России

В общем случае в нашей стране при решении задач защиты информации должно обеспечиваться соблюдение следующих указов Президента, федеральных законов, постановлений Правительства Российской Федерации, РД Гостехкомиссии России и других нормативных документов.

РД Гостехкомиссии России составляют основу нормативной базы в области защиты от НСД к информации в нашей стране. Наиболее значимые из них, определяющие критерии для оценки защищенности АС (СВТ), рассматриваются ниже.

Критерии для оценки механизмов защиты программно-технического уровня, используемые при анализе защищенности АС и СВТ, выражены в РД Гостехкомиссии РФ «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» и «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации».

РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»

РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. (Основным «источником вдохновения» при разработке этого документа послужила знаменитая американская «Оранжевая книга»). Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс седьмой, самый высокий — первый. Классы подразделяются на четыре группы, отличающиеся уровнем защиты:

Первая группа содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;

Вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;

Третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

Четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации»

РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС — коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.

Методика анализа защищенности

В настоящее время не существует каких-либо стандартизированных методик анализа защищенности АС, поэтому в конкретных ситуациях алгоритмы действий аудиторов могут существенно различаться. Однако типовую методику анализа защищенности корпоративной сети предложить все-таки возможно. И хотя данная методика не претендует на всеобщность, ее эффективность многократно проверена на практике.

Типовая методика включает использование следующих методов:

• Изучение исходных данных по АС;

• Оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов АС;

• Анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих
нормативных документов, а также их адекватности существующим

рискам;

• Ручной анализ конфигурационных файлов маршрутизаторов, МЭ и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS серверов, а также других критических элементов сетевой инфраструктуры;

• Сканирование внешних сетевых адресов ЛВС из сети Интернет;

• Сканирование ресурсов ЛВС изнутри;

• Анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств.

Перечисленные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты. Активное тестирование системы защиты заключается в эмуляции действий потенциального злоумышленника по преодолению механизмов защиты. Пассивное тестирование предполагает анализ конфигурации ОС и приложений по шаблонам с использованием списков проверки. Тестирование может производиться вручную либо с использованием специализированных программных средств.

Исходные данные по обследуемой АС

В соответствии с требованиями РД Гостехкомиссии при проведении работ по аттестации безопасности АС, включающих в себя предварительное обследование и анализ защищенности объекта информатизации, заказчиком работ должны быть предоставлены следующие исходные данные:

1. Полное и точное наименование объекта информатизации и его назначение.
2. Характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) информации и уровень секретности (конфиденциальности) обрабатываемой информации определен (в соответствии с какими перечнями (государственным, отраслевым, ведомственным, предприятия).
3. Организационная структура объекта информатизации.
4. Перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация.
5. Особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны.
6. Структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации,

используемые протоколы обмена информацией.
7.Общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации.
8.Наличие и характер взаимодействия с другими объектами информатизации.
9.Состав и структура системы защиты информации на аттестуемом объекте информатизации.
10. Перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию.
11.Сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ.
12 Наличие на объекте информатизации (на предприятии, на котором расположен объект информатизации) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных).
13. Наличие и основные характеристики физической защиты объекта информатизации помещений, где обрабатывается защищаемая информация и хранятся информационные носители).
14 Наличие и готовность проектной и эксплуатационной документации на объект информатизации **и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.**

Анализ конфигурации средств защиты внешнего периметра ЛВС

При анализе конфигурации средств защиты внешнего периметра ЛВС и управления межсетевыми взаимодействиями особое внимание обращается на следующие аспекты, определяемые их конфигурацией:

- Настройка правил разграничения доступа (правил фильтрации сетевых пакетов) на МЭ и маршрутизаторах;
- Используемые схемы и настройка параметров аутентификации;
- Настройка параметров системы регистрации событий;
- Использование механизмов, обеспечивающих сокрытие топологии защищаемой сети,
  включающих в себя трансляцию сетевых адресов (NAT) и маскарадинг;

- Настройка механизмов оповещения об атаках и реагирования;
- Наличие и работоспособность средств контроля целостности;
- Версии используемого ПО и наличие установленных пакетов программных коррекций.

Методы тестирования системы защиты

Тестирование системы защиты АС проводится с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости в отношении возможных атак, а также с целью поиска уязвимостей в защите. Традиционно используются два основных метода тестирования:

- тестирование по методу «черного ящика»;
- тестирование по методу «белого ящика».

Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. При этом против объекта испытаний реализуются все известные типы атак и проверяется устойчивость системы защиты в отношении этих атак. Используемые методы тестирования эмулируют действия потенциальных злоумышленников, пытающихся взломать систему защиты. Основным средством тестирования в данном случае являются сетевые сканеры, располагающие базами данных известных уязвимостей.

Метод «белого ящика» предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяются наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рисками. Выводы о наличие уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного ПО, а затем проверяются на практике. Основным инструментом анализа в данном случае являются программные агенты средств анализа защищенности системного уровня, рассматриваемые ниже

Сетевые сканеры

Основным фактором, определяющим защищенность АС от угроз безопасности, является наличие в АС уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов АС, так и другими причинами, в число которых входят

ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их неправильное использование, либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты АС, в конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости.

Сетевые сканеры являются, пожалуй, наиболее доступными и широко используемыми средствами анализа защищенности. Основной принцип их функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Сканер является необходимым инструментом в арсенале любого администратора либо аудитора безопасности АС.

Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с начала 80-х и не потерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования.

Современный сетевой сканер выполняет четыре основные задачи:

- Идентификацию доступных сетевых ресурсов;
- Идентификацию доступных сетевых сервисов;
- Идентификацию имеющихся уязвимостей сетевых сервисов;
- Выдачу рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы.

Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

В настоящее время существует большое количество как коммерческих, так и свободно распространяемых сканеров, как

универсальных, так и специализированных, предназначенных для выявления только определенного класса уязвимостей.

Механизмы работы сканеров безопасности

Существует два основных механизма, при помощи которых сканер безопасности проверяет наличие уязвимости - сканирование (scan) и зондирование (probe) [6]

.

Сканирование - механизм пассивного анализа, с помощью которого сканер пытается определить наличие уязвимости без фактического подтверждения ее наличия - по косвенным признакам. Этот метод является наиболее быстрым и простым для реализации. В терминах компании ISS данный метод получил название "логический вывод" (inference). Согласно компании Cisco этот процесс идентифицирует открытые порты, найденные на каждом сетевом устройстве, и собирает связанные с портами заголовки (banner), найденные при сканировании каждого порта. Каждый полученный заголовок сравнивается с таблицей правил определения сетевых устройств, операционных систем и потенциальных уязвимостей. На основе проведенного сравнения делается вывод о наличии или отсутствии уязвимости.

Зондирование - механизм активного анализа, который позволяет убедиться, присутствует или нет на анализируемом узле уязвимость. Зондирование выполняется путем имитации атаки, использующей проверяемую уязвимость. Этот метод более медленный, чем "сканирование", но почти всегда гораздо более точный, чем он. В терминах компании ISS данный метод получил название "подтверждение" (verification). Согласно компании Cisco этот процесс использует информацию, полученную в процессе сканирования ("логического вывода"), для детального анализа каждого сетевого устройства. Этот процесс также использует известные методы реализации атак для того, чтобы полностью подтвердить предполагаемые уязвимости и обнаружить другие уязвимости, которые не могут быть обнаружены пассивными методами, например подверженность атакам типа "отказ в обслуживании" ("denial of service").

ГЛАВА 4. Современные технологии защиты корпоративных сетей. Межсетевые экраны, системы обнаружения атак и виртуальные частные сети

МЭ называют локальное или функционально распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и/или выходящей из автоматизированной системы. МЭ основное название, определенное в РД Гостехкомиссии РФ, для данного устройства. Также встречаются общепринятые названия брандмауэр и firewall (англ. огненная стена). В строительной сфере брандмауэром (нем. brand – пожар, mauer – стена) называется огнеупорный барьер, разделяющий отдельные блоки в многоквартирном доме и препятствующий распространению пожара. МЭ выполняет подобную функцию для компьютерных сетей.

По определению МЭ служит контрольным пунктом на границе двух сетей. В самом распространенном случае эта граница лежит между внутренней сетью организации и внешней сетью, обычно сетью Интернет. Однако в общем случае, МЭ могут применяться для разграничения внутренних подсетей корпоративной сети организации.

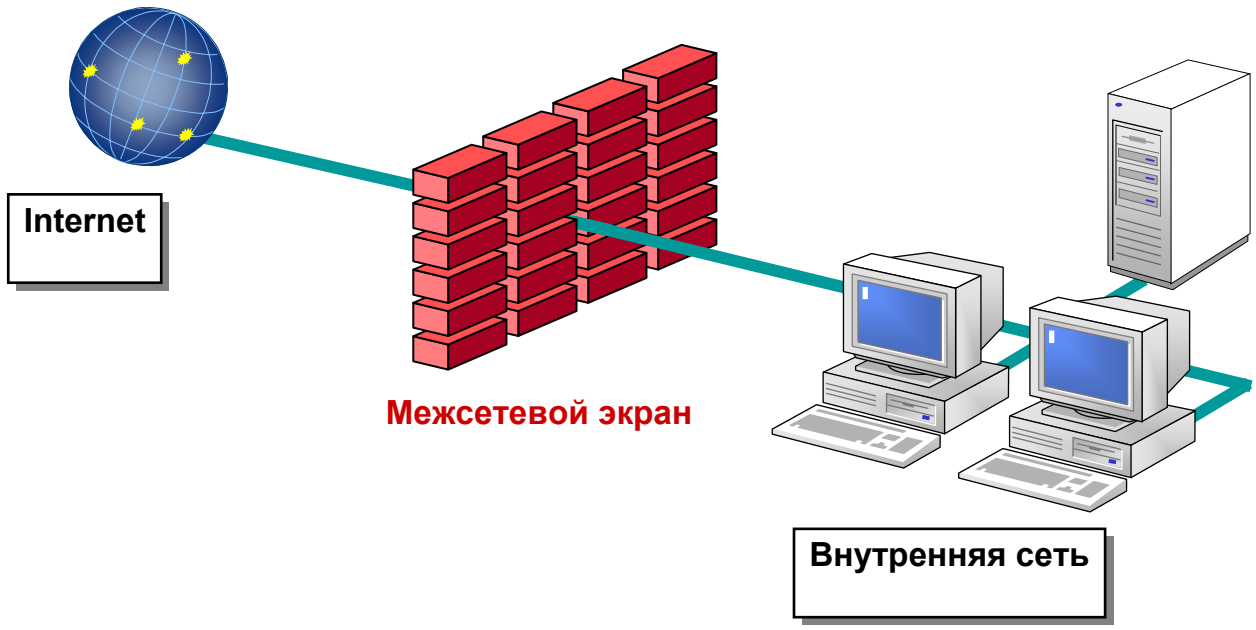

Рисунок 18. Типовое размещение МЭ в корпоративной сети

Задачами МЭ, как контрольного пункта, являются:

- Контроль всего трафика, ВХОДЯЩЕГО во внутреннюю корпоративную сеть
- Контроль всего трафика, ИСХОДЯЩЕГО из внутренней корпоративной сети

Контроль информационных потоков состоит в их фильтрации и преобразовании в соответствие с заданным набором правил. Поскольку в современных МЭ фильтрация может осуществляться на разных уровнях эталонной модели взаимодействия открытых систем (ЭМВОС, OSI), МЭ удобно представить в виде системы фильтров. Каждый фильтр на основе анализа проходящих через него данных, принимает решение – пропустить дальше, перебросить за экран, блокировать или преобразовать данные.

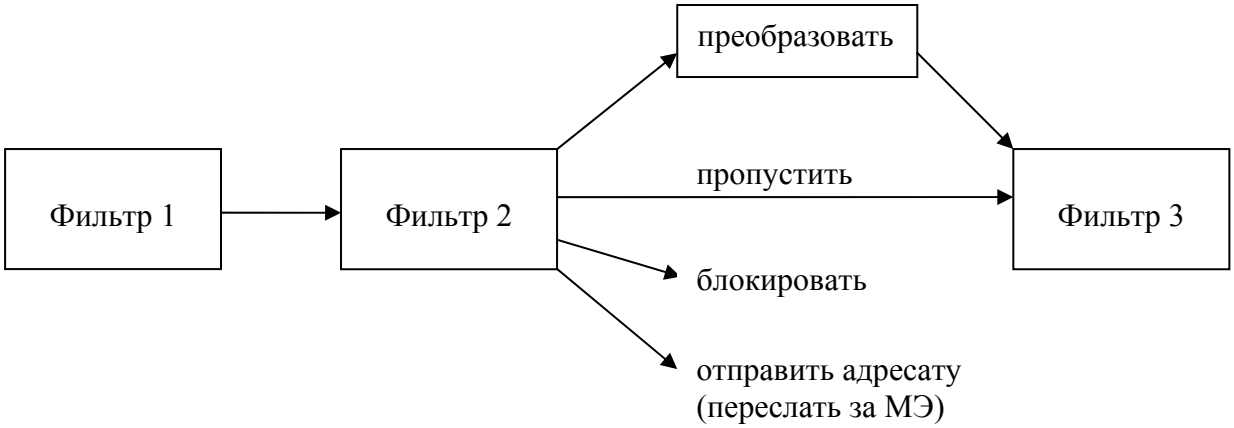

Рисунок 19. Схема фильтрации в МЭ.

Неотъемлемой функцией МЭ является **протоколирование** информационного обмена. Ведение журналов регистрации позволяет администратору выявить подозрительные действия, ошибки в конфигурации МЭ и принять решение об изменении правил МЭ.

Классификация МЭ

Выделяют следующую классификацию МЭ, в соответствие с функционированием на разных уровнях МВОС (OSI):

- Мостиковые экраны (2 уровень OSI)
- Фильтрующие маршрутизаторы (3 и 4 уровни OSI)
- Шлюзы сеансового уровня (5 уровень OSI)
- Шлюзы прикладного уровня (7 уровень OSI)

- Комплексные экраны (3-7 уровни OSI)

Рассмотрим данные категории подробнее.

Мостиковые МЭ

Данный класс МЭ, функционирующий на 2-м уровне модели OSI, известен также как прозрачный (stealth), скрытый, теневой МЭ. Мостиковые МЭ появились сравнительно недавно и представляют перспективное направление развития технологий межсетевого экранирования. Фильтрация трафика ими осуществляется на канальном уровне, т.е. МЭ работают с фреймами (frame, кадр).

К достоинствам подобных МЭ можно отнести:

- Нет необходимости в изменении настроек корпоративной сети, не требуется дополнительного конфигурирования сетевых интерфейсов МЭ.
- Высокая производительность. Поскольку это простые устройства, они не требуют больших затрат ресурсов. Ресурсы требуются либо для повышения возможностей машин, либо для более глубокого анализа данных.
- Прозрачность. Ключевым для этого устройства является его функционирование на 2 уровне модели OSI. Это означает, что сетевой интерфейс не имеет IP-адреса. Эта особенность более важна, чем легкость в настройке. Без IP-адреса это устройство не доступно в сети и является невидимым для окружающего мира. Если такой МЭ недоступен, то как его атаковать? Атакующие даже не будут знать, что существует МЭ, проверяющий каждый их пакет.

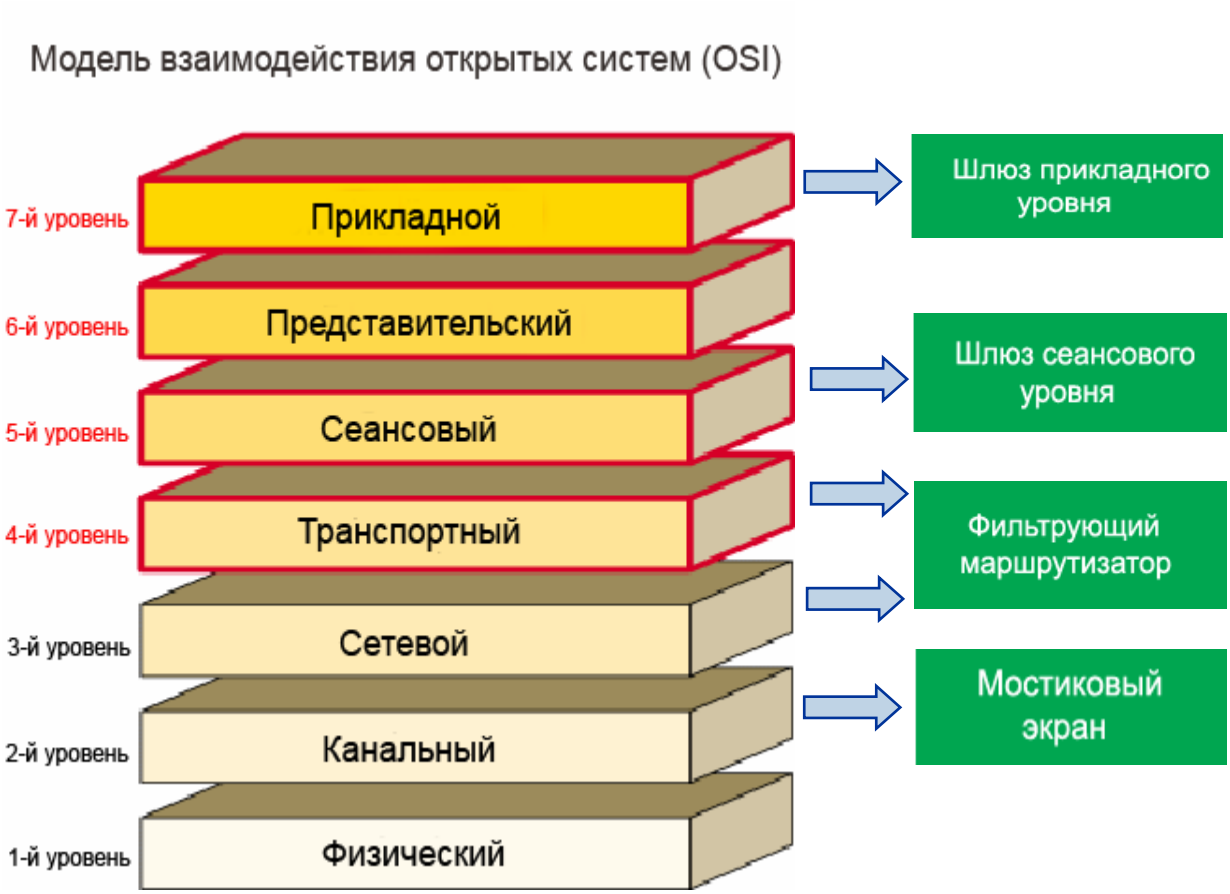

Рисунок 20. Фильтрация трафика МЭ на разных уровнях МВОС.

Фильтрующие маршрутизаторы

Packet-filtering firewall (Межсетевой экран с фильтрацией пакетов) — межсетевой экран, который является маршрутизатором или компьютером, на котором работает программное обеспечение, сконфигурированное таким образом, чтобы отфильтровывать определенные виды входящих и исходящих пакетов. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP-заголовках пакетов (адреса отправителя и получателя, их номера портов и др.)

- Работают на 3 уровне
- Также известны, как МЭ на основе порта
- Каждый пакет сравнивается со списками правил (адрес источника/получателя, порт источника/получателя)
- Недорогой, быстрый (производительный в силу простоты), но наименее безопасный
- Технология 20-летней давности

- Пример: список контроля доступа (ACL, access control lists) маршрутизатора

Шлюз сеансового уровня

Circuit-level gateway (Шлюз сеансового уровня) — межсетевой экран, который исключает прямое взаимодействие между авторизированным клиентом и внешним хостом. Сначала он принимает запрос доверенного клиента на определенные услуги и, после проверки допустимости запрошенного сеанса, устанавливает соединение с внешним хостом. После этого шлюз просто копирует пакеты в обоих направлениях, не осуществляя их фильтрации. На этом уровне появляется возможность использования функции сетевой трансляции адресов (NAT, network address translation). Трансляция внутренних адресов выполняется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов IP-адреса компьютеров-отправителей внутренней сети автоматическип преобразуются в один IP-адрес, ассоциируемый с экранирующим МЭ. В результате все пакеты, исходящие из внутренней сети, оказываются отправленными МЭ, что исключает прямой контакт между внутренней и внешней сетью. IP-адрес шлюза сеансового уровня становится единственным активным IP-адресом, который попадает во внешнюю сеть.

- Работает на 4 уровне
- Передает TCP подключения, основываясь на порте
- Недорогой, но более безопасный, чем фильтр пакетов
- Вообще требует работы пользователя или программы конфигурации для полноценной работы
- Пример: SOCKS файрвол

Шлюз прикладного уровня

Application-level gateways (Шлюз прикладного уровня) - межсетевой экран, который исключает прямое взаимодействие между авторизированным клиентом и внешним хостом, фильтруя все входящие и исходящие пакеты на прикладном уровне модели OSI. Связанные с приложением программы-посредники перенаправляют через шлюз информацию, генерируемую конкретными сервисами TCP/IP.
Возможности:

- Идентификация и аутентификация пользователей при попытке установления соединения через МЭ;
- Фильтрация потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;
- Регистрация событий и реагирование на события;
- Кэширование данных, запрашиваемых из внешней сети.

На этом уровне появляется возможность использования функций посредничества (Proxy).

Для каждого обсуживаемого протокола прикладного уровня можно вводить программных посредников – HTTP-посредник, FTP-посредник и т.д. Посредник каждой службы TCP/IP ориентирован ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе. Также, как и шлюз сеансового уровня, прикалдной шлюз перехватывает с помощью соотвествующих экранирующих агентов входящие и сходящие пакеты, копирует и перенаправляет информацию через шлюз, и функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетью. Однако, посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уровня. Во-первых, посредники прикладного шлюза связаны с конкретными приложениями программными серверами), а во-вторых, они могут фильтровать поток сообщений на прикладном уровне модели МВОС.

Особенности:

- Работает на 7 уровне
- Специфический для приложений
- Умеренно дорогой и медленный, но более безопасный и допускает регистрацию деятельности пользователей
- Требует работы пользователя или программы конфигурации для полноценной работы
- Пример: Web (http) proxy

МЭ экспертного уровня

Stateful inspection firewall — межсетевой экран экспертного уровня, который проверяет содержимое принимаемых пакетов на трех уровнях модели OSI: сетевом, сеансовом и прикладном. При выполнении этой задачи используются специальные алгоритмы фильтрации пакетов, с помощью которых каждый пакет сравнивается с известным шаблоном авторизированных пакетов.

- Фильтрация 3 уровня
- Проверка правильности на 4 уровне
- Осмотр 5 уровня
- Высокие уровни стоимости, защиты и сложности
- Пример: CheckPoint Firewall-1

Некоторые современные МЭ используют комбинацию вышеперечисленных методов и обеспечивают дополнительные способы защиты, как сетей, так и систем.

«Персональные» МЭ

Этот класс МЭ позволяет далее расширять защиту, допуская управление по тому, какие типы системных функций или процессов имеют доступ к ресурсам сети. Эти МЭ могут использовать различные типы сигнатур и условий, для того, чтобы разрешать или отвергать трафик. Вот некоторые из общих функций персональных МЭ:

- Блокирование на уровне приложений – позволять лишь некоторым приложениям или библиотекам исполнять сетевые действия или принимать входящие подключения
- Блокирование на основе сигнатуры – постоянно контролировать сетевой трафик и блокировать все известные атаки.

Дополнительный контроль увеличивает сложность управления безопасностью из-за потенциально большого количества систем, которые могут быть защищены персональным файрволом. Это также увеличивает риск повреждения и уязвимости из-за плохой настройки

Динамические МЭ

Динамические МЭ объединяют в себе стандартные МЭ (перечислены выше) и методы обнаружения вторжений, чтобы обеспечить блокирование «на лету» сетевых подключений, которые соответствуют определённой сигнатуре, позволяя при этом подключения от других источников к тому же самому порту. Например, можно блокировать деятельность сетевых червей, не нарушая работу нормального трафика.

Политика работы МЭ

МЭ функционируют по одному из двух принципов:

- запрещать все, что не разрешено в явной форме
- разрешать все, что не запрещено в явной форме

Схемы подключения МЭ

- Схема единой защиты локальной сети
- Схема защищаемой закрытой и не защищаемой открытой подсетями
- Схема с раздельной защитой закрытой и открытой подсетей.

Схема единой защиты локальной сети

Наиболее простым является решение, при котором межсетевой экран просто экранирует локальную сеть от глобальной. При этом WWW-сервер, FTP-сервер, почтовый сервер и другие сервера, оказываются также защищены межсетевым экраном. При этом требуется уделить много внимания на предотвращение проникновения на защищаемые станции локальной сети при помощи средств легкодоступных WWW-серверов.

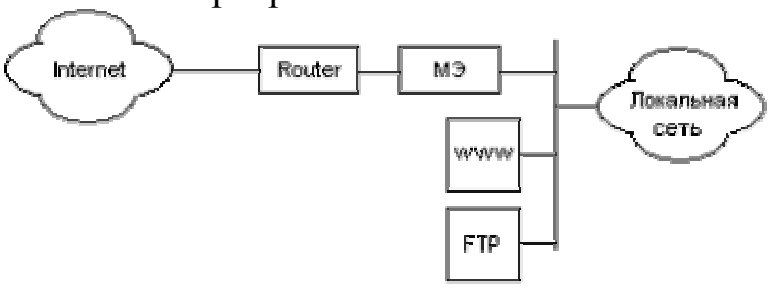

Рисунок 21. Схема единой защиты локальной сети.

Схема защищаемой закрытой и не защищаемой открытой подсетями

Для предотвращения доступа в локальную сеть, используя ресурсы WWW-сервера, рекомендуется общедоступные серверы подключать перед межсетевым экраном. Данный способ обладает более высокой защищенностью локальной сети, но низким уровнем защищенности WWW- и FTP-серверов.

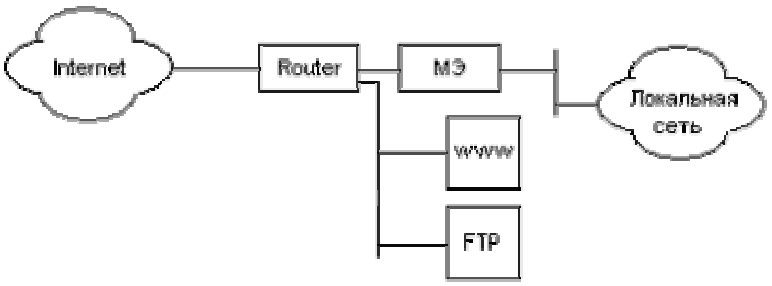

Рисунок 22. Схема защищаемой закрытой и не защищаемой открытой подсетями

Схема с раздельной защитой закрытой и открытой подсетей

Данная схема подключения обладает наивысшей защищенностью по сравнению с рассмотренными выше. Схема основана на применении двух МЭ, защищающих отдельно закрытую и открытую подсети. Участок сети между МЭ также называется экранированной подсетью или демилитаризованной зоной (DMZ, demilitarized zone).

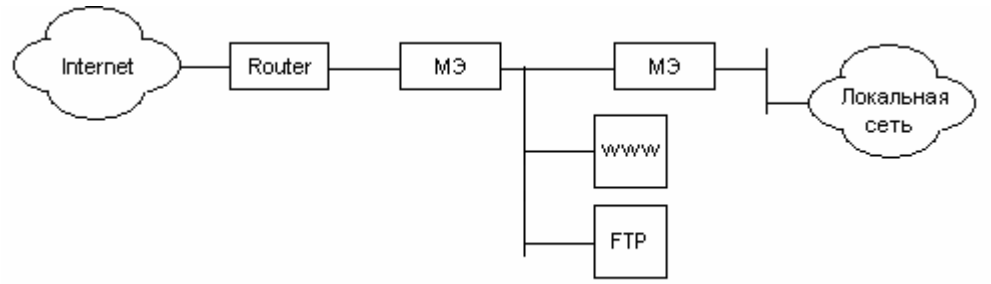

Схема 23. Схема с раздельной защитой закрытой и открытой подсетей

Системы обнаружения атак

Наряду со стандартными средствами защиты, без которых немыслимо нормальное функционирование АС (таких как МЭ, системы резервного копирования и антивирусные средства), существует необходимость использования СОА (IDS, систем обнаружения атак или вторжений), которые являются основным средством борьбы с сетевыми атаками [7].

В настоящее время СОА начинают все шире внедряться в практику обеспечения безопасности корпоративных сетей. Однако существует ряд проблем, с которыми неизбежно сталкиваются организации, развертывающие у себя систему выявления атак. Эти проблемы существенно затрудняют, а порой и останавливают процесс внедрения IDS. Вот некоторые из них:

- высокая стоимость коммерческих СОА;

- невысокая эффективность современных СОА, характеризующаяся большим числом ложных срабатываний и несрабатываний (false positives and false negatives);
- требовательность к ресурсам и порой неудовлетворительная производительность СОА уже на 100 Мбит/с сетях;
- недооценка рисков, связанных с осуществлением сетевых атак;
- отсутствие в организации методики анализа и управления рисками, позволяющей адекватно оценивать величину риска и обосновывать стоимость реализации контрмер для руководства;
- высокая квалификация экспертов по выявлению атак, требующаяся для внедрения и развертывания СОА.

Специфичной для России также является относительно невысокая зависимость информационной инфраструктуры предприятий от Интернет и финансирование мероприятий по обеспечению информационной безопасности по остаточному принципу, что не способствует приобретению дорогостоящих средств защиты для противодействия сетевым атакам.

Тем не менее, процесс внедрения СОА в практику обеспечения информационной безопасности продолжается, в том числе и в России.

Типовая архитектура системы выявления атак, как правило, включает в себя следующие компоненты:

1. Сенсор (средство сбора информации);
2. Анализатор (средство анализа информации);
3. Средства реагирования;
4. Средства управления.

Конечно, все эти компоненты могут функционировать и на одном компьютере и даже в рамках одного приложения, однако чаще всего они территориально и функционально распределены. Такие компоненты СОА, как анализаторы и средства управления, опасно размещать за МЭ во внешней сети, т. к. если они будут скомпрометированы, то злоумышленник может получить доступ к информации о структуре внутренней защищаемой сети на основе анализа базы правил, используемой СОА.

Типовая архитектура системы выявления атак изображена на рисунке. Сетевые сенсоры осуществляют перехват сетевого трафика, хостовые сенсоры используют в качестве источников информации журналы регистрации событий ОС, СУБД и приложений. Информация о событиях также может быть получена хостовым сенсором непосредственно от ядра ОС, МЭ или приложения. Анализатор, размещаемый на сервере безопасности, осуществляет централизованный сбор и анализ информации, полученной от сенсоров.

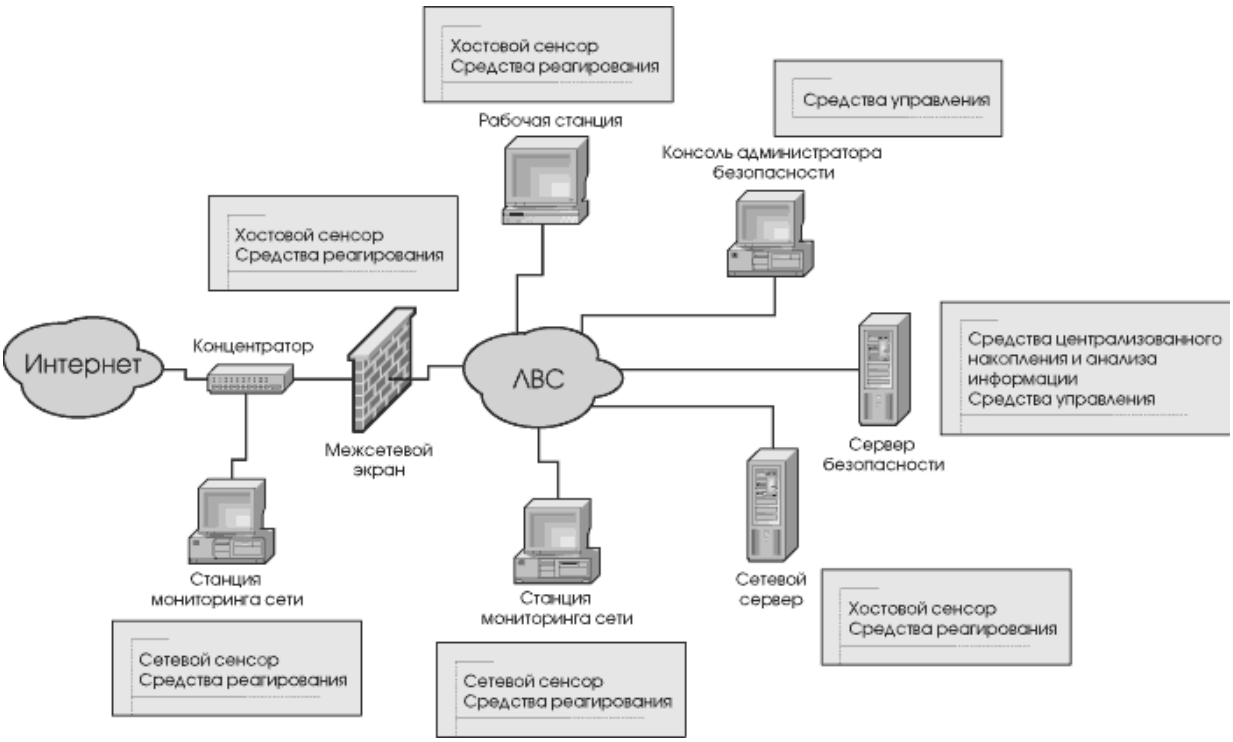

Рисунок 24. Типовая архитектура СОА.

Средства реагирования могут размещаться на станциях мониторинга сети, МЭ, серверах и рабочих станциях ЛВС. Типичный набор действий по реагированию на атаки включает в себя оповещение администратора безопасности (средствами электронной почты, вывода сообщения на консоль или отправки на пэйджер), блокирование сетевых сессий и пользовательских регистрационных записей с целью немедленного прекращения атак, а также протоколирование действий атакующей стороны.

Средства управления предназначены для администрирования всех компонентов системы выявления атак, разработки алгоритмов выявления и реагирования на нарушения безопасности (политик безопасности), а также для просмотра информации о нарушениях и генерации отчетов.

Виртуальные частные сети

В связи с широким распространением Internet, intranet, extranet при разработке и применении распределенных информационных сетей и

систем одной из самых актуальных задач является решение проблем информационной безопасности [8].

В последнее десятилетие в связи с бурным развитием Internet и сетей коллективного доступа в мире произошел качественный скачок в распространении и доступности информации. Пользователи получили дешевые и доступные каналы связи. Стремясь к экономии средств, предприятия используют такие каналы для передачи критичной коммерческой информации. Однако принципы построения Internet открывают злоумышленникам возможности кражи или преднамеренного искажения информации. Не обеспечена достаточно надежная защита от проникновения нарушителей в корпоративные и ведомственные сети.

Для эффективного противодействия сетевым атакам и обеспечения возможности активного и безопасного использования в бизнесе открытых сетей в начале 90-х годов родилась и активно развивается концепция построения защищенных виртуальных частных сетей - VPN. (Virtual Private Networks).

Концепция построения защищенных виртуальных частных сетей VPN

В основе концепции построения защищенных виртуальных частных сетей VPN лежит достаточно простая идея: если в глобальной сети есть два узла, которые хотят обменяться информацией, то для обеспечения конфиденциальности и целостности передаваемой по открытым сетям информации между ними необходимо построить виртуальный туннель, доступ к которому должен быть чрезвычайно затруднен всем возможным активным и пассивным внешним наблюдателям. Термин «виртуальный» указывает на то, что соединение между двумя узлами сети не является постоянным (жестким) и существует только во время прохождения трафика по сети.

Преимущества, получаемые компанией при формировании таких виртуальных туннелей, заключаются, прежде всего, в значительной экономии финансовых средств.

Функции и компоненты сети VPN

Защищенной виртуальной сетью VPN называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю

среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

При подключении корпоративной локальной сети к открытой сети возникают угрозы безопасности двух основных типов:

- несанкционированный доступ к корпоративным данным в процессе их передачи по открытой сети;
- несанкционированный доступ к внутренним ресурсам корпоративной локальной сети, получаемый злоумышленником в результате несанкционированного входа в эту сеть.

Защита информации в процессе передачи по открытым каналам связи основана на выполнении следующих основных функций:

- аутентификации взаимодействующих сторон;
- криптографическом закрытии (шифровании) передаваемых данных;
- проверке подлинности и целостности доставленной информации.

Для этих функций характерна взаимосвязь друг с другом. Их реализация основана на использовании криптографических методов защиты информации.

Для защиты локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды обычно используют межсетевые экраны, поддерживающие безопасность информационного взаимодействия путем фильтрации двустороннего потока сообщений, а также выполнения функций посредничества при обмене информацией. Межсетевой экран располагают на стыке между локальной и открытой сетью. Для защиты отдельного удаленного компьютера, подключенного к открытой сети, программное обеспечение межсетевого экрана устанавливают на этом же компьютере, и такой межсетевой экран называется персональным.

Туннелирование

Защита информации в процессе ее передачи по открытым каналам основана на построении защищенных виртуальных каналов связи, называемых криптозащищенными туннелями. Каждый такой туннель представляет собой соединение, проведенное через открытую сеть, по

которому передаются криптографически защищенные пакеты сообщений.
Создание защищенного туннеля выполняют компоненты виртуальной сети, функционирующие на узлах, между которыми формируется туннель. Эти компоненты принято называть инициатором и терминатором туннеля. Инициатор туннеля инкапсулирует (встраивает) пакеты в новый пакет, содержащий наряду с исходными данными новый заголовок с информацией об отправителе и получателе. Хотя все передаваемые по туннелю пакеты являются пакетами IP, инкапсулируемые пакеты могут принадлежать к протоколу любого типа, включая пакеты немаршрутизируемых протоколов, таких, как NetBEUI. Маршрут между инициатором и терминатором туннеля определяет обычная маршрутизируемая сеть IP, которая может быть и сетью отличной от Интернет. Терминатор туннеля выполняет процесс обратный инкапсуляции – он удаляет новые заголовки и направляет каждый исходный пакет в локальный стек протоколов или адресату в локальной сети.

Сама по себе инкапсуляция никак не влияет на защищенность пакетов сообщений, передаваемых по туннелю. Но благодаря инкапсуляции появляется возможность полной криптографической защиты инкапсулируемых пакетов. Конфиденциальность инкапсулируемых пакетов обеспечивается путем их криптографического закрытия, то есть зашифровывания, а целостность и подлинность – путем формирования цифровой подписи. Поскольку существует большое множество методов криптозащиты данных, очень важно, чтобы инициатор и терминатор туннеля использовали одни и те же методы и могли согласовывать друг с другом эту информацию. Кроме того, для возможности расшифровывания данных и проверки цифровой подписи при приеме инициатор и терминатор туннеля должны поддерживать функции безопасного обмена ключами. Ну и наконец, чтобы туннели создавались только между уполномоченными пользователями, конечные стороны взаимодействия требуется аутентифицировать.

Классификация виртуальных частных сетей VPN

Наиболее часто используются следующие три признака классификации VPN:

- рабочий уровень модели OSI;
- конфигурация структурно-технического решения;

- способ технической реализации.

Классификация VPN по рабочему уровню ЭМВОС

Для технологий безопасной передачи данных по общедоступной (незащищенной) сети применяют обобщенное название - *защищенный канал* (secure channel).

Защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях эталонной модели взаимодействия открытых систем (ЭМВОС, OSI) (рис.25).

<table>
<tr><td rowspan="7">Протоколы защищенного доступа</td><td>Прикладной</td><td rowspan="2">Влияют на приложения</td></tr>
<tr><td>Представительный</td></tr>
<tr><td>Сеансовый</td><td></td></tr>
<tr><td>Транспортный</td><td rowspan="4">Прозрачны для приложений</td></tr>
<tr><td>Сетевой</td></tr>
<tr><td>Канальный</td></tr>
<tr><td>Физический</td></tr>
</table>

Рис.25. Уровни протоколов защищенного канала

От выбранного уровня OSI во многом зависит функциональность реализуемой VPN и ее совместимость с приложениями ИС, а также с другими средствами защиты. По признаку рабочего уровня модели OSI различают следующие группы VPN:

- VPN второго (канального) уровня;
- VPN третьего (сетевого) уровня;
- VPN пятого (сеансового) уровня.

VPN строятся на достаточно низких уровнях модели OSI. Причина этого в том, что чем ниже в стеке реализованы средства защищенного канала, тем проще их сделать прозрачными для приложений и прикладных протоколов. Однако здесь возникает другая проблема - зависимость протокола защиты от конкретной сетевой технологии.

Если для защиты данных используется протокол одного из верхних уровней (прикладного или представительного), то такой способ защиты не зависит от того, какие сети (IP или IPX, Ethernet или ATM) применяются для транспортировки данных, что можно считать несомненным достоинством. С другой стороны, приложение при этом

становится зависимым от конкретного протокола защиты, то есть для приложений подобный протокол не является прозрачным.

Защищенному каналу на самом высоком, прикладном уровне свойствен еще один недостаток = ограниченная область действия. Протокол защищает только вполне определенную сетевую службу - файловую, гипертекстовую или почтовую. Например, протокол S/MIME защищает исключительно сообщения электронной почты. Поэтому для каждой службы необходимо разрабатывать соответствующую защищенную версию протокола.

На верхних уровнях модели OSI существует жесткая связь между используемым стеком протоколов и приложением.

VPN канального уровня

Средства VPN, используемые на канальном уровне модели OSI, позволяют обеспечить инкапсуляцию различных видов трафика третьего уровня (и более высоких уровней) и построение виртуальных туннелей типа «точка-точка» (от маршрутизатора к маршрутизатору или от персонального компьютера к шлюзу ЛВС). К этой группе относятся VPN-продукты, которые используют протоколы L2F (Layer 2 Forwarding) и PPTP (Point-to-Point Tunneling Protocol), а также сравнительно недавно утвержденный стандарт L2TP (Layer 2 Tunneling Protocol), разработанный совместно фирмами Cisco Systems и Microsoft.

Протокол защищенного канала PPTP основан на протоколе PPP и обеспечивает прозрачность средств защиты для приложений и служб прикладного уровня. Протокол PPTP может переносить пакеты как в сетях IP, так и в сетях, работающих на основе протоколов IPX, DECnet или NetBEUI.

Протокол L2TP используется при организации удаленного доступа к ЛВС (поскольку базируется в основном на ОС Windows). Между тем решения второго уровня не приобретут, вероятно, такое же значение для взаимодействия ЛВС, по причине недостаточной масштабируемости при необходимости иметь несколько туннелей с общими конечными точками.

VPN сетевого уровня

VPN-продукты сетевого уровня выполняют инкапсуляцию IP в IP. Одним из широко известных протоколов на этом уровне является SKIP, который постепенно вытесняется новым протоколом IPSec,

предназначенным для аутентификации, туннелирования и шифрования IP-пакетов.

Работающий на сетевом уровне протокол IPSec представляет компромиссный вариант. С одной стороны, он прозрачен для приложений, а с другой, может работать практически во всех сетях, так как основан на широко распространенном протоколе IP.

Протокол IPSec предусматривает стандартные методы идентификации пользователей или компьютеров при инициации туннеля, стандартные способы использования шифрования конечными точками туннеля, а также стандартные методы обмена и управления ключами шифрования между конечными точками.

Протокол IPSec может работать совместно с L2TP; в результате эти два протокола обеспечивают более надежную идентификацию, стандартизованное шифрование и целостность данных. Туннель IPSec между двумя локальными сетями может поддерживать множество индивидуальных каналов передачи данных, в результате чего приложения данного типа получают преимущества с точки зрения масштабирования.

Говоря об IPSec, необходимо упомянуть протокол (IKE) позволяющий защитить передаваемую информацию от постороннего вмешательства. Он решает задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами.

VPN сеансового уровня

Некоторые VPN используют другой подход под названием «посредники каналов» (circuit proxy). Этот метод функционирует над транспортным уровнем и ретранслирует трафик из защищенной сети в общедоступную сеть Internet для каждого сокета в отдельности. (Протокол IP не имеет пятого - сеансового - уровня, однако ориентированные на сокеты операции часто называют операциями сеансового уровня.)

Шифрование информации, передаваемой между инициатором и терминатором туннеля часто осуществляется с помощью защиты транспортного уровня TLS.

Для стандартизации аутентифицированного прохода через межсетевые экраны консорциум IETF определил протокол под названием SOCKS, и в настоящее время протокол SOCKS v.5 применяется для стандартизованной реализации посредников каналов.

В протоколе SOCKS v.5 клиентский компьютер устанавливает аутентифицированный сокет (или сеанс) с сервером, выполняющим роль посредника (proxy). Этот посредник - единственный способ связи через межсетевой экран. Посредник, в свою очередь, проводит любые операции, запрашиваемые клиентом. Поскольку посреднику известно о трафике на уровне сокета, он может осуществлять тщательный контроль, например блокировать конкретные приложения пользователей, если они не имеют необходимых полномочий.

Классификация VPN по архитектуре технического решения

По архитектуре технического решения принято выделять три основных вида виртуальных частных сетей:

- VPN с удаленным доступом;
- внутрикорпоративные VPN;
- межкорпоративные VPN.

Виртуальные частные сети VPN с удаленным доступом (Remote Access) предназначены для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам мобильным и/или удаленным (home-office) сотрудникам компании.

Внутрикорпоративные сети VPN (intranet-VPN) предназначены для обеспечения защищенного взаимодействия между подразделениями внутри предприятия или между группой предприятий, объединенных корпоративными сетями связи, включая выделенные линии.

Межкорпоративные сети VPN (extranet-VPN) обеспечивают сотрудникам предприятия защищенный обмен информацией со стратегическими партнерами по бизнесу, поставщиками, крупными заказчиками, пользователями, клиентами и т.д.

Extranet-VPN обеспечивает прямой доступ из сети одной компании к сети другой, тем самым способствуя повышению надежности связи, поддерживаемой в ходе делового сотрудничества. В межкорпоративных сетях большое значение придается контролю доступа посредством межсетевых экранов и аутентификации пользователей.

Классификация VPN по способу технической реализации

По способу *технической* реализации различают следующие группы V.PN:

- VPN на основе сетевой операционной системы;
- VPN на основе межсетевых экранов;
- VPN на основе маршрутизаторов;
- VPN на основе программных решений;
- VPN на основе специализированных аппаратных средств со встроенными шифропроцессорами.

VPN на основе сетевой ОС

Реализацию VPN на основе сетевой ОС можно рассмотреть на примере операционной системы Windows NT. Для создания VPN компания Microsoft предлагает протокол PPTP, интегрированный в сетевую операционную систему Windows NT. Такое решение выглядит привлекательно для организаций, использующих Windows в качестве корпоративной ОС. В сетях VPN, основанных на Windows NT, используется база данных клиентов, хранящаяся в контроллере PDC (Primary Domain Controller). При подключении к PPTP-серверу пользователь авторизуется по протоколам PAP, CHAP или MS CHAP. Для шифрования применяется нестандартный фирменный протокол Point-to-Point Encryption с 40-битовым ключом, получаемым при установлении соединения.

В качестве достоинства приведенной схемы следует отметить, что стоимость решения на основе сетевой ОС значительно ниже стоимости других решений

Несовершенство такой системы - недостаточная защищенность протокола PPTP.

VPN на основе маршрутизаторов

Данный способ построения VPN предполагает применение маршрутизаторов для создания защищенных каналов. Поскольку вся информация, исходящая из локальной сети, проходит через маршрутизатор, то вполне естественно возложить на него и задачи шифрования.

VPN на основе межсетевых экранов

Межсетевые экраны большинства производителей содержат функции туннелирования и шифрования данных. К программному обеспечению собственно межсетевого экрана добавляется модуль шифрования.

К недостаткам этого метода относятся высокая стоимость решения в пересчете на одно рабочее место и зависимость производительности от аппаратного обеспечения, на котором работает межсетевой экран. При использовании межсетевых экранов на базе ПК надо помнить, что подобный вариант подходит только для небольших сетей с ограниченным объемом передаваемой информации.

VPN на основе программного обеспечения

Для построения сетей VPN также применяются программные решения. При реализации подобных схем используется специализированное ПО, работающее на выделенном компьютере и в большинстве случаев выполняющее функции proxy-сервера. Компьютер с таким программным обеспечением может быть расположен за межсетевым экраном,

.

VPN на основе специализированных аппаратных средств со встроенными шифропроцессорами

Вариант построения VPN на специализированных аппаратных средствах может быть использован в сетях, требующих высокой производительности. Недостаток подобного решения - его высокая стоимость.

Технические и экономические преимущества внедрения технологий VPN в корпоративные сети

Технология виртуальных частных сетей VPN позволяет эффективно решать задачи, связанные с циркуляцией конфиденциальной информации по каналам связи. Она обеспечивает связь между сетями, а также между удаленным пользователем и корпоративной сетью с помощью защищенного канала (туннеля), «проложенного» в общедоступной сети Internet.

Таким образом, на современном этапе развития, в условиях, когда филиалы одного и того же предприятия находятся на значительном удалении друг от друга, потребность в оперативном и надежном обмене информацией стала наиболее острой. Использование дорогих высокопропускных каналов связи не всегда оказывается целесообразным и экономически выгодным. Развитие же средств связи, особенно недорогих и наиболее доступных (например, Internet), приводит к тому, что их практическое использование, особенно пред-приятиями, становится все более массовым. В этих условиях становится

заманчивым их использование для передачи ценной корпоративной информации, убытки от потери или искажения которой могут пагубно сказаться на деятельности компании. Поэтому использование защищенных виртуальных частных сетей VPN с учетом всех их достоинств становится все более актуальным и жизненно необходимым. Концепция таких сетей позволяет организовывать столь необходимый обмен информацией внутри компании и с клиентами при наилучшем сочетании производительности, оперативности, защищенности и стоимости. Надо предположить, что такие технологии, как VPN, будут активно развиваться, совершенствоваться и приобретать все более массовый характер.

ГЛАВА 5. Внутренние злоумышленники в корпоративных сетях. Методы воздействия.

Вопреки распространенному мнению о том, что основную опасность для компании представляют внешние нарушители, действующие из сети Интернет, так называемые хакеры, реальная угроза современной компании исходит от внутренних нарушителей. По многочисленным исследованиям около 70-80% всех нарушений в корпоративной среде приходится на долю внутренних нарушителей.

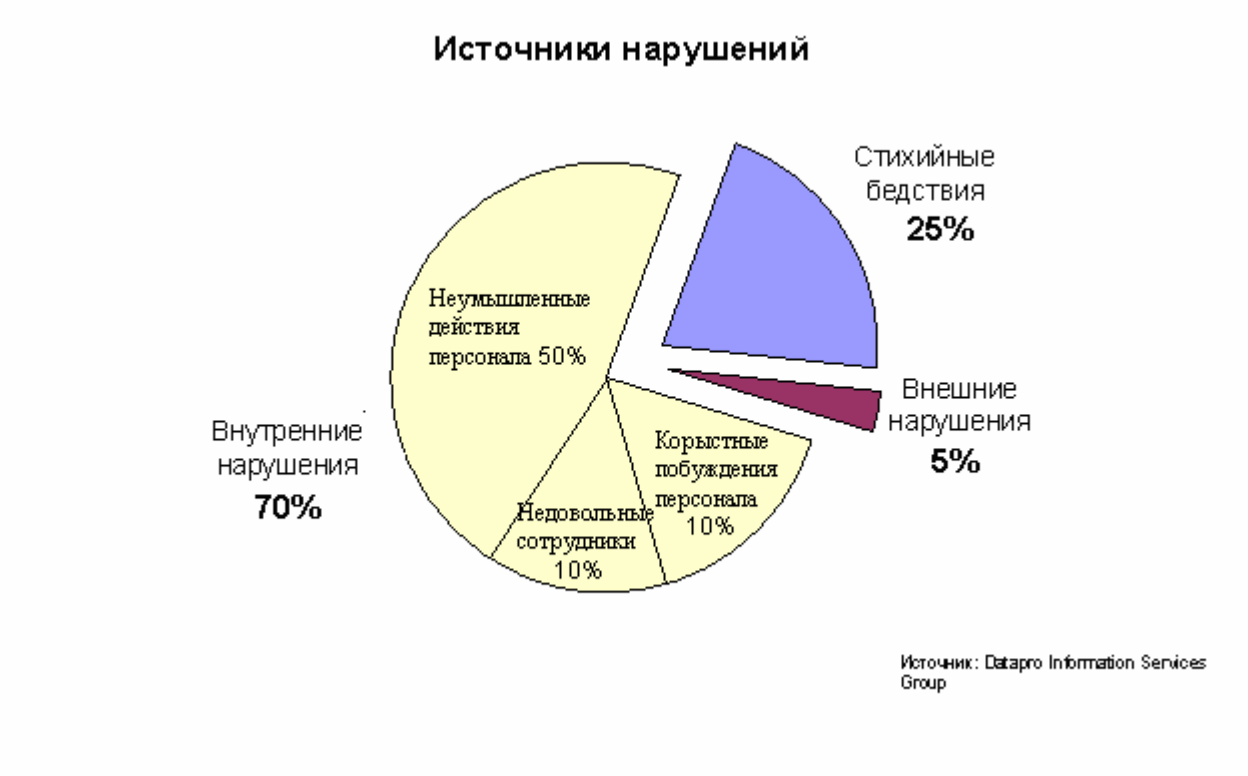

Рисунок 26. Источники нарушений в современной компании

Нарушителем в общем смысле является лицо, по ошибке, незнанию или осознанно предпринявшее попытку выполнения запрещенных операций и использующее для этого различные возможности, методы и средства. Внутренний нарушитель представляет собой легитимного сотрудника организации, имеющего определенный доступ к ее информационным ресурсам. Причем, причинами нарушений внутри организации могут быть как ошибки персонала, так и умышленные действия с их стороны. Таким образом, согласно общемировой статистике на долю внутренних нарушителей, умышленно совершающих противоправные действия, приходится около 20% всех инцидентов в компании, в то время как внешние нарушители повинны только в 5% подобных случаев. В данной главе рассмотрены возможные

действия внутренних злоумышленников внутри корпоративной сети и предложены меры противодействия.

В отечественной и зарубежной компьютерной литературе применяется различная терминология в отношении компьютерных преступников. Отсутствие единой классификации часто приводит к путанице. Так, «хакером» (hacker) чаще всего называют именно компьютерных злоумышленников, а иногда – высококвалифицированных компьютерных специалистов. Последних еще иногда называют «белыми шляпами» (white-hats), в отличие от «черных шляп», цель которых нанести вред системе. Также часто используются понятия кракер (cracker), kid-hacker, spy и т.д. Наиболее полная классификация приведена в [9]. Во избежание путаницы здесь и далее применяются термины «нарушитель» и «злоумышленник» (intruder), для обобщенного обозначения тех, кто умышленно совершает нарушения в корпоративную сеть [10]. Нарушители могут быть разбиты на две категории:

Outsiders (англ. чужой, посторонний) - это нарушители из сети Интернет, которые атакуют внутренние ресурсы корпоративной сети (удаление информации на корпоративном веб-сервере, пересылка спама через почтовый сервер и т.д.) и которые обходят МЭ и СОА для того, чтобы проникнуть во внутреннюю корпоративную сеть. Злоумышленники могут атаковать из Интернет, через модемные линии, через физическое подключение к каналам связи или из сети партнеров (поставщиков, заказчиков, дилеров и т.д.).

Insiders (англ. свой, хорошо осведомленный человек) - это те, кто находится внутри корпоративной сети, и имеют определенный доступ к корпоративным серверам и рабочим станциям. Они включают пользователей, неправильно использующих свои привилегии, или исполняющих роль привилегированного пользователя (например, с привилегированного терминала). Эти люди изначально находятся в преимущественном положении, чем Outsiders. Поскольку они уже владеют конфиденциальной информацией о фирме, недоступной для внешних нарушителей. В отличие от внешних нарушителей, для которых в общем случае атакуемая корпоративная сеть изначально представляет «черный ящик», внутренние нарушители – это люди, которые знают, как работает фирма, и понимают ее слабости. Знают, что пароль у шефа записан на бумажке, которая лежит у него на столе, что пароль секретарши – имя ее собачки, знают, когда администратор идет пить чай и т.д.

Так по статистике наибольшая часть преступлений против банков совершается с использованием так называемой «инсайдерской» информации [11].

Еще несколько примеров. В феврале 2001 года двое бывших сотрудников компании Commerce One, воспользовавшись украденным паролем администратора, удалили с сервера файлы, составлявшие крупный (на несколько миллионов долларов) проект для иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери ограничились расходами на следствие и средства защиты от подобных инцидентов в будущем. В августе 2002 года преступники предстали перед судом.

Кража 3 миллионов долларов была совершена из банка Стокгольма, с использованием привилегированного положения нескольких служащих в информационной системе банка и также оказалась успешной [12].

Таким образом, проблема защита от внутренних нарушителей находится в центре внимания данной лекции. Именно эта проблема является сейчас наиболее актуальной и менее исследованной. Если в обеспечении защиты от внешних нарушителей давно уже выработаны устоявшиеся подходы (хотя развитие происходит и здесь), то методы противодействия внутренним нарушителям в настоящее время имеют много нерассмотренных вопросов. В частности, не имеется ясного представления о методах работы внутренних нарушителей.

Модель внутреннего нарушителя

Исследование проблем защиты корпоративных сетей целесообразно начать с рассмотрения модели потенциального нарушителя.

По оценкам специалистов в настоящее время около 70-90% интеллектуального капитала компании хранится в цифровом виде – текстовых файлах, таблицах, базах данных. Использование информационных технологий предоставляет значительные преимущества для бизнеса, однако приводит и к появлению новых угроз. По причине недостаточного серьезного отношения руководства к информационной безопасности, недобросовестным сотрудникам предоставляются широкие возможности несанкционированного доступа к информации компании, составляющей коммерческую тайну и имеющую реальную или потенциальную экономическую ценность.

Рассмотрим, при каких условиях легального сотрудника организации можно назвать внутренним нарушителем. Для эффективного функционирования организации необходимо, чтобы в ней имелась общая стратегия деятельности и четкие должностные

инструкции каждому сотруднику. Следующим организационным документом должна быть **политика безопасности** организации, в которой изложены принципы организации и конкретные меры по обеспечению информационной безопасности предприятия. *Классификационный раздел* политики безопасности описывает имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты. В *штатном разделе* приводятся описания должностей с точки зрения информационной безопасности. Наконец, раздел, описывающий *правила разграничения доступа к корпоративной информации,* является ключевым для определения внутреннего нарушителя [13].

Любое нарушение легальным сотрудником политики безопасности организации автоматически делает его внутренним нарушителем. Подобные действия можно разделить на умышленные и неумышленные. Неумышленные действия вызваны недостатком квалификации пользователей и в данной работе не рассматриваются. Умышленные действия различаются по целям: направленные на получение конфиденциальной информации вне рамок основной деятельности и связанные с нарушением распорядка работы.

Однако исследование, проведенное компанией Gartner Group показало, что 85% современных компаний не имеют ни концепции, ни политики безопасности [14]. И хотя ситуация должна измениться – по прогнозам Gartner к 2005 году таких компаний будет только 50%, следует внести коррективы в формулировку внутреннего нарушителя. Таким образом, для большинства компаний внутреннего нарушителя нельзя определить, как лицо, нарушающее политику безопасности, так как последняя просто отсутствует. Поэтому в подобном случае внутренним нарушителем, действующим умышленно, будем считать сотрудника компании, предпринимающего направленные попытки получения, изменения или уничтожения конфиденциальных данных организации вне рамок основной деятельности сотрудника.

Примерами таких действий могут быть:

- Несанкционированный доступ к данным о клиентах и сотрудниках организации вне рамок основной деятельности;
- Попытки изменения статуса пользователя;
- Попытки подбора паролей в защищенные приложения, области дискового пространства;
- Умышленные действия, связанные с попытками изменения информационного наполнения системы:
- Умышленные действия, направленные на деструкцию системы;

- Внедрение аппаратных и программных "закладок" и "вирусов", позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам сети;

Руководствуясь РД Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», определим квалификацию предполагаемого внутреннего нарушителя [15]. Будем предполагать, что нарушитель по уровню возможностей в системе относится к 3-му уровню. Третий уровень определяется возможностью управления функционированием автоматизированных систем, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования. 4-му, и самому высокому, уровню соответствует системный администратор или администратор безопасности, чьи возможности в системе максимальны по определению. По образному выражению одного из экспертов по информационной безопасности компании ISS, сетевой администратор – это «серый кардинал» компании, которому доступна практически вся информация в организации. Поэтому мы ограничиваемся рассмотрением 3-го уровня, когда нарушитель в пределах своей рабочей станции имеет широкие возможности по модификации программного обеспечения и аппаратной части.

Отметим что, согласно рассматриваемому РД, в своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты. Данное предположение позволяет более адекватно оценивать возможные угрозы. Например, в компаниях, занимающихся предоставлением услуг информационной безопасности, большинство сотрудников являются квалифицированными техническими специалистами.

При создании модели нарушителя и оценке риска потерь от действий персонала необходимо дифференцировать всех сотрудников по их возможностям доступа к системе и, следовательно, по потенциальному ущербу от каждой категории пользователей. Например, оператор или программист может нанести несравненно больший ущерб, чем обычный пользователь, тем более непрофессионал.

Ниже приводится *примерный* список персонала типичной корпоративной сети и соответствующая степень риска от каждого из них [16]:

1. Наибольший риск:

- сетевой администратор;
- администратор безопасности.

2. Повышенный риск:

- оператор системы;
- оператор ввода и подготовки данных;
- менеджер обработки;
- системный программист.

3. Средний риск:
- инженер системы;
- менеджер программного обеспечения.

4. Ограниченный риск:
- прикладной программист;
- инженер или оператор по связи;
- администратор баз данных;
- инженер по оборудованию;
- оператор периферийного оборудования;
- библиотекарь системных магнитных носителей;
- пользователь-программист;
- пользователь-операционист.

5. Низкий риск:
- инженер по периферийному оборудованию;
- библиотекарь магнитных носителей пользователей;
- пользователь сети.

Каждый из перечисленных выше пользователей в соответствии со своей категорией риска может нанести больший или меньший ущерб системе.

Мы не рассматриваем здесь вопросы мотивации сотрудников, побуждающие их совершать противоправные действия. Однако отметим, что чаще всего причинами являются: работа на компанию-конкурента, любопытство, месть руководству компании.

Модель типовой корпоративной сети

Рассмотрение возможных действий злоумышленников необходимо вести в условиях, существующих в современных отечественных компаниях. Рассмотрим типовую корпоративную сеть, построенную на аппаратных и программных средствах, широко использующихся в корпоративных сетях частных и государственных организаций.

Аппаратные средства корпоративных сетей включают физическую среду и оборудование передачи данных. Вследствие ограниченного применения в настоящее время (по крайней мере, в России) беспроводных сетей, типовая корпоративная сеть построена на основе кабельной системы, представляющей собой витую пару 5-й категории. Современные корпоративные сети разрабатываются с применением

коммутаторов (switch) и концентраторов (hub). Оба этих сетевых устройства служат для объединения компьютеров в локальные сети. Хотя концентраторы в настоящее время вытесняются коммутаторами, тем не менее, во многих сетях организаций концентраторы широко используются в силу своей дешевизны. Коммутатор представляет собой более сложное сетевое устройство. И как следствие различаются по набору поддерживаемых функций. Наиболее сложные (и дорогие) модели называются управляемыми интеллектуальными коммутаторами и обладают собственным IP-адресом, поддержкой удаленного администрирования, средствами организации виртуальных сетей (VLAN) и развитым набором средств защиты. Стоимость интеллектуальных коммутаторов может достигать 2000 долларов, что затрудняет их покупку небольшими организациям. Программные средства, используемые в типовой сети, также являются стандартными для большинства организаций. Рабочие станции на базе операционных систем (ОС) Windows 95, 98, NT4 Workstation, 2000, XP (по статистике в 90% всех организаций в мире используются рабочие станции на базе Windows разных версий). Сервера на базе ОС Windows NT4 Server/Terminal Server Edition, 2000 Server, 2003 Server. Пакеты популярного программного обеспечения (ПО) для офисной работы: 1С, MS Outlook, MS Office 97/2000/XP. Серверное ПО: 1С, MS SQL Server, MS Exchange.

В качестве средств защиты используются межсетевые экраны: Agnitum Outpost Firewall, Kerio Personal Firewall, Kaspersky Anti-Hacker, Norton Personal Firewall; системы обнаружения атак Black ICE, Snort, RealSecure.

Методы воздействий нарушителя на корпоративную сеть

Нарушитель изучает объект нападения как теоретически, так и практически. Практическое исследование объекта и его системы безопасности может быть пассивным и активным. Пассивным воздействием называют воздействие, не оказывающее непосредственного влияния на работу корпоративной сети, но которое может нарушать ее политику безопасности. Ввиду отсутствия непосредственного влияния на работу сети, такое воздействие очень трудно обнаружить. Примером пассивного воздействия является прослушивание канала связи.

Активные воздействия предполагают непосредственное влияние на работу корпоративной сети и нарушают действующую в ней политику

безопасности. В результате активных действий в системе происходят определенные изменения. Поэтому активные воздействия легче обнаружить, чем пассивные.

Рисунок 27. Методы воздействия внутреннего нарушителя на корпоративную сеть.

Пассивные методы воздействия

Прослушивание сетевого трафика

Рассмотрим возможность прослушивания канала связи (sniffing) в локальной сети организации. Для прослушивания трафика необходимо перевести сетевой адаптер в «беспорядочный» (promiscuous) режим. В данном режиме адаптер перехватывает все сетевые пакеты, проходящие через него, а не только предназначенные данному адресу, как в нормальном режиме функционирования. Если локальная сеть построена на концентраторах, то для злоумышленника оказывается доступным весь сетевой трафик в пределах сегмента локальной сети. В сети построенной на коммутаторах, трафик направляется только тому компьютеру, которому он предназначен. То есть если компьютер "A" обменивается пакетами с компьютером "B", то компьютер "C" не способен перехватывать этот трафик. Однако, существует ряд технологий позволяющих обойти ограничения, накладываемые коммутаторами. Эти технологии – ARP Spoofing (ARP-poisoning), MAC Flooding и MAC Duplicating [17]. Рассмотрим их подробнее.

Метод **ARP-Spoofing** основан на атаке «человек посередине» (man-in-the-middle).

Данная атака возможна из-за уязвимости в реализации протокола ARP. Протокол разрешения адресов ARP (Address Resolution Protocol) предназначен для выяснения MAC-адреса хоста по его IP-адресу. Для обмена информацией двум хостам в сети Ethernet, каждому из них необходимо получить MAC-адрес другого. Эта процедура осуществляется с использованием протокола ARP. Хост «A», желающий установить соединение с хостом «B», сначала проверяет наличие MAC-адреса хоста «B» в своем ARP-кэше. В случае его отсутствия в кэше, осуществляется рассылка широковещательного запроса с целью выявить MAC-адрес, соответствующий IP-адресу хоста «B». Хост «B», сравнив IP-адрес в запросе со своим IP-адресом, посылает ответ (ARP-reply), в который помещает свой MAC-адрес. Оба хоста «A» и «B» помещают полученные MAC-адреса в свои ARP-кэши, чтобы минимизировать количество широковещательных запросов. Теперь хосты могут обмениваться данными, используя MAC-адреса.

Атаку на данный информационный обмен возможно произвести, потому что протокол ARP не требует аутентификации. Для реализации атаки злоумышленнику с хоста «C» необходимо послать обоим хостам сгенерированные ARP-reply пакеты:

- для хоста «A», в котором прописано, что IP-адресу хоста «B» соответствует MAC-адрес хоста «C»;
- для хоста «B», в котором прописано, что IP-адресу хоста «A» соответствует MAC-адрес хоста «C».

Хосты «A» и «B» в соответствии со спецификацией протокола ARP, получив подобные reply-пакеты, обновят свои ARP-кэши. Теперь, пакеты, отправляемые хостом «A» хосту «B» будут фактически отсылаться хосту «C», поскольку в ARP-кэше хоста «A» IP-адресу хоста «B» соответствует MAC-адрес хоста «C». Поэтому данная атака получила также название ARP-poisoning (отравление ARP-кэша). Для нормальной передачи пакетов между хостами «A» и «B» хосту «C» необходимо выполнять функции роутера для данных хостов, т.е. организовать их передачу по маршрутам A-C-B и B-C-A.

Отметим некоторые особенности реализации данной атаки:

- так как протокол ARP функционирует только рамках одной широковещательной подсети, атаку ARP-spoofing нельзя провести для хостов в разных подсетях или виртуальных локальных вычислительных сетях (VLAN);
- поскольку операционная система хостов периодически обновляет ARP-кэш, хосту «C» необходимо периодически выполнять процедуру «отравления кэша» для хостов «A» и «B»;
- в случае прослушивания трафика между некоторым хостом и роутером сети, в результате получается, что злоумышленник сможет прослушивать трафик между данным хостом и любым хостом в Интернет.

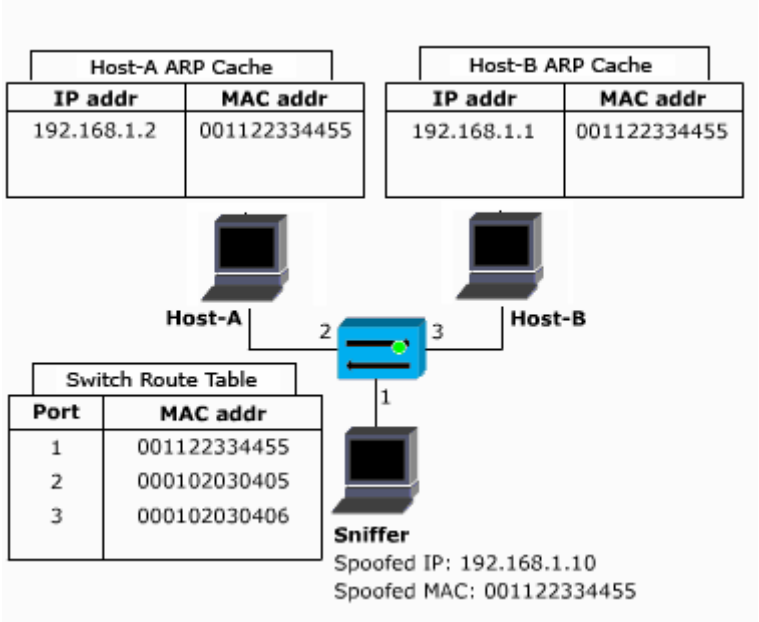

Рисунок 28. Демонстрация атаки ARP-spoofing (источник: www.oxid.it)

Следует отметить, что если на коммутаторе не включена функция Port-Security (данная функция будет рассмотрена позже), то можно в качестве MAC-адреса сниффера использовать любой MAC-адрес.

Атака **MAC-duplicating** заключается в установке на хосте злоумышленника «C» MAC-адреса, совпадающего с MAC-адресом другого хоста в сети, например «B». Теперь все пакеты, направляемые хосту «B» будут также посланы и хосту «C». Задача злоумышленника не отвечать на эти пакеты, а только принимать их.

Атака **MAC-flooding** основана на особенности работы коммутаторов. Посылка на коммутатор огромного числа ARP-запросов на несуществующие IP-адреса, вызовет переполнение памяти коммутатора и его переход в режим функционирования концентратора. Для обратного перехода в нормальный режим функционирования необходимо перегрузить питание коммутатора.

Таким образом, реализуя атаки ARP-Spoofing и MAC-duplicating, можно прослушивать трафик между любыми хостами в локальной сети корпорации, построенной на концентраторах и коммутаторах без использования шифрования.

Перехват сетевого трафика осуществляется с использованием специального ПО – сетевых мониторов. Надо отметить, что не все сетевые мониторы могут перехватывать весь проходящий через них сетевой трафик. Например, Microsoft Network Monitor в стандартной комплектации Windows NT/2000/XP/2003, отображает пакеты, адресованные только данному компьютеру. В то же время, существует множество альтернативных сетевых мониторов, из которых самыми богатыми по набору функций являются Sniffer Pro от компании NAI, IRIS Network Traffic Analyzer от компании eEYE и TCP Dump. Интересной программой также является утилита Cain & Abel 2.5 итальянского специалиста по сетевой безопасности Massimiliano Montoro, включающая в себя много полезных для администраторов функций. Отметим, что подавляющему большинству снифферов для перехвата всего сетевого трафика требуется установить специальные драйвера, для чего требуются администраторские права в ОС. Однако существуют снифферы, не требующих никаких специализированных

драйверов, например, NGSSniff от компании NGSS Inc., который может осуществлять захват, используя Windows Sockets.

Исследуем, к каким последствиям может привести прослушивание сетевого трафика. Современные сетевые протоколы локальных и глобальных сетей разрабатывались, когда проблемы информационной безопасности не являлись первоочередными. Соответственно, в данных протоколах практически отсутствую механизмы защиты. Это справедливо для многих широко-используемых протоколов – TCP/IP, ARP, HTTP, FTP, SMTP, POP3 и т.д. Поэтому в последние 5-10 лет были разработаны усовершенствованные версии протоколов передачи данных, способных противостоять угрозам безопасности. Однако по ряду причин переход на более защищенные протоколы затянулся. Так уже несколько лет ведутся дискуссии о переходе от использования в Интернет протокола IPv4 к IPv6, включающего спецификацию IPSec для защиты передаваемых данных. А в корпоративных сетях по-прежнему используются незащищенные протоколы. Рассмотрим уязвимости этих протоколов важные применительно к корпоративным сетям.

Основными слабостями сетевых протоколов является отсутствие средств обеспечения конфиденциальности передаваемых данных. Так, при наличии в корпоративной сети почтового сервера с доступом по протоколам POP3, SMTP и IMAP, злоумышленник, перехватывающий трафик между почтовым сервером и любым узлом сети (например, компьютером директора), может завладеть аутентификационными данными пользователя. Это возможно, так как согласно спецификации протокола POP3 [18] аутентификационные данные передаются в открытом виде. Использование данной уязвимости иллюстрирует следующий рисунок (рис 29).

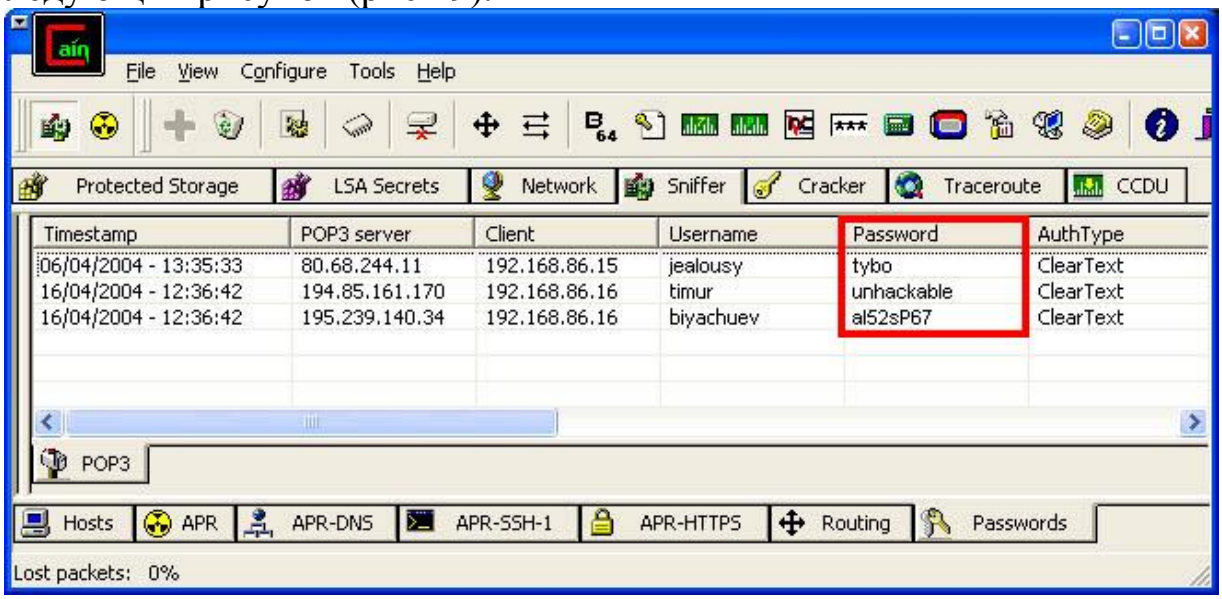

Рисунок 29. Экранный снимок программы Cain & Abel, перехватившей почтовые пароли.

Таким образом, внутренний нарушитель, используя специальное ПО, может получить пароли всех пользователей к корпоративному почтовому серверу. В результате злоумышленник сможет читать любую корпоративную переписку, а также писать письма от имени других пользователей. Так же можно использовать скомпрометированную почтовую учетную запись для выноса из корпоративной сети конфиденциальной информации. Например, используя учетную запись какого-либо служащего переслать внутренние конфиденциальные материалы на временный бесплатный электронный ящик в Интернете.

Однако существуют более серьезные последствия перехвата почтовых учетных записей. При использовании почтовых серверов на базе Microsoft Exchange в сетях построенных на базе домена Windows NT/2000, при создании пользователя, сразу же создается почтовый ящик с теми же именем пользователя и паролем, что и для доступа к домену Windows NT. В результате, перехват аутентификационных данных почтового сервера позволяет злоумышленнику получить доступ к домену от имени другого лица, например, своего непосредственного начальника. А, скомпрометировав компьютер администратора сети, можно получить практически неограниченный доступ к ее информационным ресурсам.

Зная доменные аутентификационные данные пользователя или администратора домена, злоумышленник может получить практически полный доступ к данным, хранящимся на локальных машинах. В ОС Windows 2000/XP/Server при запущенной службе доступа к файлам и принтерам (file and printer sharing), функционирующей по протоколу NetBIOS, в настройках по умолчанию для доступа из сети открыты все диски компьютера (под администраторским паролем). Данная функция реализована для административных нужд, однако она предоставляет значительную опасность. Зная аутентификационные данные пользователя компьютера, если компьютер не входит в домен, или администратора домена, если компьютер включен в домен, можно получить неограниченный доступ к файловым ресурсам компьютера.

Так же скомпрометированным окажется и файловый сервер – основное хранилище конфиденциальной информации компании. Поскольку доступ к файловому серверу Windows, функционирующему чаще всего по протоколу NetBIOS, также осуществляется по аутентификационным данным домена.

В случае использования в корпоративной сети файлового FTP-сервера, возможен перехват аутентификационных данных и в этом

случае. В спецификации протокола FTP также не предусмотрено скрытие параметров аутентификации [19].

Использование внутреннего Web-сервера в корпорации с разграничением доступа пока не распространено. Однако и в этом случае без принятия специальных мер (например, поддержки SSL), в режиме «базовой аутентификации» по протоколу HTTP имя пользователя и его пароль передаются в открытом виде.

Также не шифруют передаваемые данные протоколы Telnet и SNMPv1.

Многие пользователи имеют бесплатные почтовые ящики в Интернете, такие как mail.ru, hotbox.com и т.д. Доступ к этим ящикам осуществляется с использованием web-интерфейса или с помощью почтовых программ, таких как Microsoft Outlook или The Bat. В большинстве случаев пользователи, не желая запоминать множество паролей, выбирают один и тот же пароль для множества служб – бесплатного почтового сервера, сервера приложений, компьютера на работе или домена. Таким образом, перехваченный злоумышленником пароль к почтовому серверу в Интернет, может предоставить ему доступ к ресурсам корпоративной сети. В подтверждение актуальности данной угрозы, приведем результаты исследования InfoSecurity 2003. Среди 152 участников исследования слово «password» в виде пароля используют 12%. Популярней только собственное имя пользователя — 16%. Дальше идут названия футбольной команды (11%) и дата рождения (8%). Устроители InfoSecurity 2003 также установили, что две трети граждане используют везде один тот же пароль: и на работе, и для банковского счета, и для электронной почты.

Следует отметить, что в настоящее время получили широкое распространение службы мгновенного обмена сообщениями (IM-службы) – ICQ, Windows Messenger, AOL и другие. Мгновенные сообщения (IM, instant messaging) - удобное дополнение, а в ряде случаев, и неплохая замена переписке по электронной почте. В отличие от электронной почты, мгновенная передача сообщений позволяет пользователю видеть - доступен ли выбранный друг или сотрудник в сети. Как правило, IM-служба дает пользователю информацию, если доступен кто-то из корреспондентов личного списка пользователя. Служба мгновенного обмена сообщениями также выгодно отличает от электронной почты возможность двустороннего обмена сообщениями практически в реальном масштабе времени. Существует огромное число пользователей такой связи, у нее масса сторонников и даже своих идеологов, доказывающих, что использование мгновенной передачи сообщений на рабочем месте вместо традиционной электронной почты ведет к более эффективной и надежной связи рабочего места и, поэтому,

к более высокой производительности труда сотрудников. В результате, IM быстро развивается и в профессиональных и в личных приложениях. По информации Ferris Research, до 70% офисных работников пользуются «ICQ» или другими IM-инструментами в деловых целях, целиком полагаясь на их надежность. Однако использование такой службы в компании приводит к появлению серьезных угроз. В частности, данные, передаваемые по сети службы мгновенной передачи сообщений, не шифруются. Так что в большинстве IM-сетей перехвата сообщений можно опять таки использовать обычный сниффер. Это особенно опасно в крупных корпорациях, так как часто личная, секретная и другая конфиденциальная информация передается по ICQ или другой IM-сети (так как существует распространенное ошибочное мнение о большей надежности именно такого способа передачи самой секретной информации).

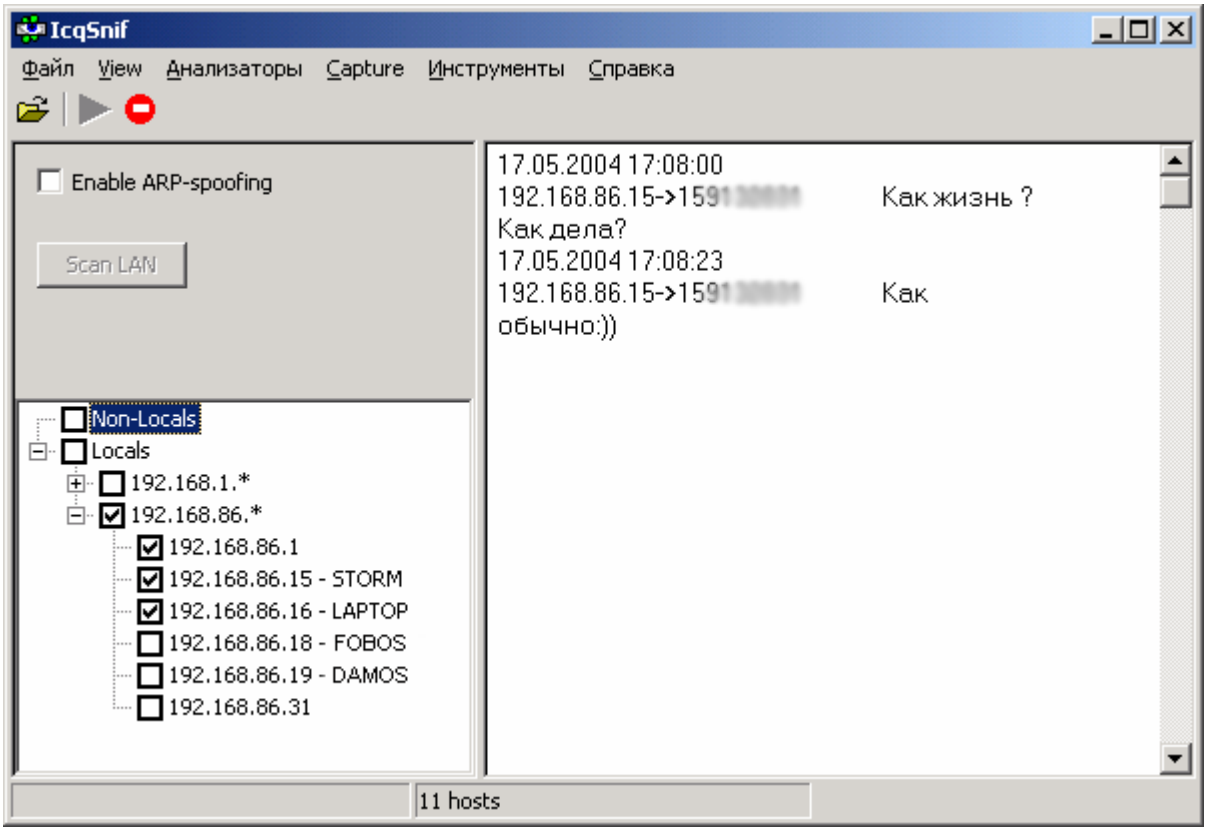

Рисунок 30. Перехват IM-сообщений с помощью программы-сниффера ICQ-сообщений ICQ Sniff (www.ufasoft.com/icqsnif) .

Мы рассмотрели уязвимости протоколов передачи данных без механизмов аутентификации и со встроенными механизмами аутентификации, а теперь исследуем защищенность протоколов сетевой аутентификации.

Аутентификация есть процесс проверки подлинности пользователя, т. е. подтверждение того, что пользователь действительно имеет учетную запись и может ее использовать при обращении к службам и ресурсам как локальным, так и сетевым. В настоящее время в сетях, построенных на базе MS Windows, применяются следующие протоколы аутентификации: LAN Manager, NTLM v.1, NTLM v.2, Kerberos. С развитием Windows компания Microsoft стремилась усилить безопасность применяемых протоколов аутентификации. Так протокол LAN Manager, обладающей очень низкой криптостойкостью был заменен протоколом NTLM v.1, который после найденных в нем уязвимостей был модифицирован до версии NTLM v.2. Однако в последствии были найдены уязвимости метода аутентификации и для этого протокола [20]. Поэтому в Windows 2000 Microsoft перешла на новый протокол проверки подлинности в сетях – Kerberos v.5, являющийся открытым промышленным стандартом. Тем не менее, были найдены уязвимости и у этого механизма аутентификации в Windows [21],[22]. Отметим, что для совместимости с предыдущими версиями Windows, в старших версиях осуществляется поддержка всех менее надежных протоколов аутентификации.

В результате, прослушивая трафик можно получить аутентификационные данные, представляющие собой права доступа к сетевым ресурсам, например, доменные учетные записи пользователей. Пароли посылаются по сети не в открытом виде, а в виде хэшей (рис 31). Таким образом, перехватив аутентификационные данные, можно попытаться восстановить по ним исходные пароли.

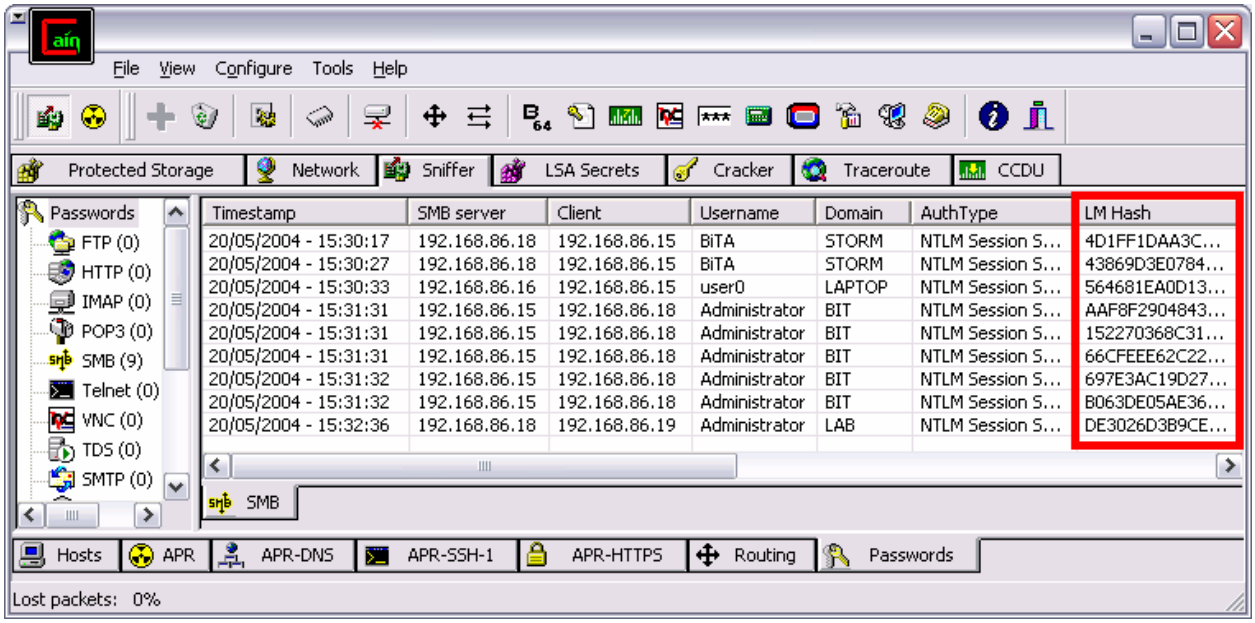

Рисунок 31. Захват данных аутентификации.

Исследуем, насколько опасна возможность перехвата паролей с точки зрения их последующего взлома. Рассмотрим два основных подхода к криптоанализу: перебор (прямой и ли по словарю) и с использованием таблиц предварительных вычислений (table precomputation).

При методе прямого перебора атакующий пробует все возможные ключи для дешифрования текста. Перебор по словарю предполагает, что пароль вероятнее всего является осмысленным словом или простой комбинацией слов, букв, цифр. Существуют специализированные словари, содержащие комбинации, наиболее часто применяемые в качестве паролей. Применение атаки по словарю позволяет значительно сократить время, требуемое для подбора паролей (рис. 32).

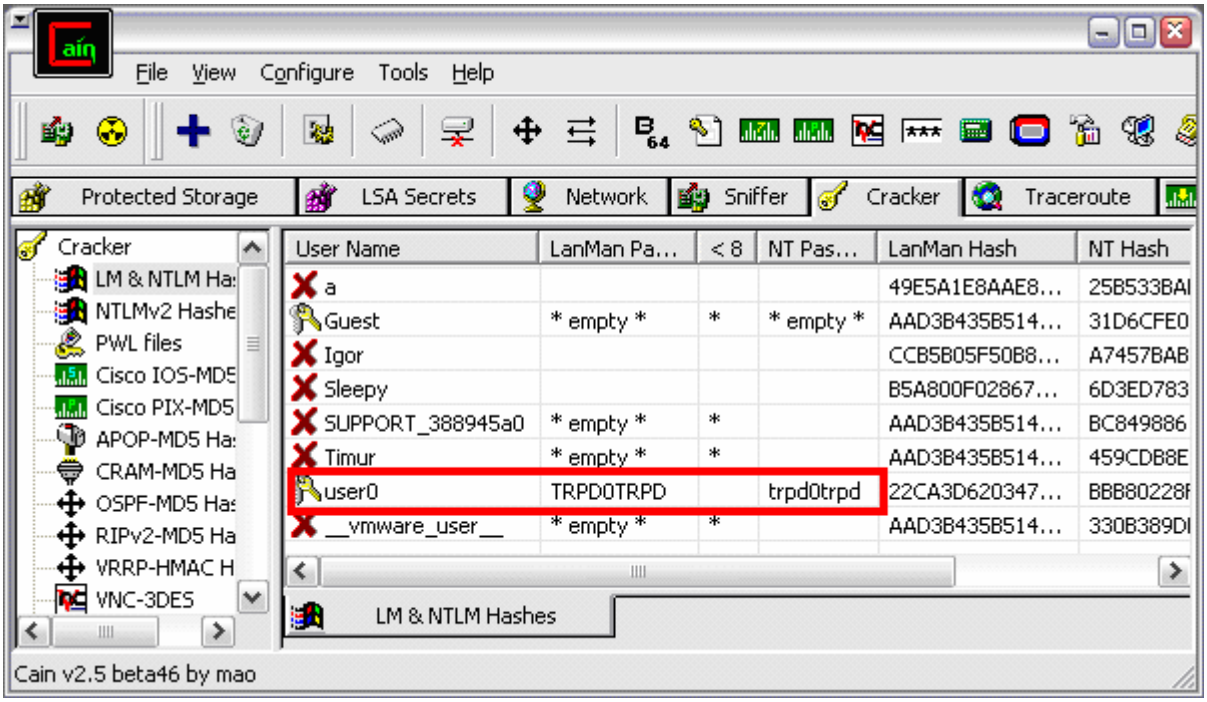

Рисунок 32. Подбор пароля пользователя User0 методом прямого перебора.

Идея таблиц предварительных вычислений состоит в том, чтобы предварительно вычислить и сохранить в таблице выборочный исходный текст и соответствующие ключи для всех возможных ключей. Впервые подобный метод предложил в 1980 году Matrin Hellman. Модифицированный швейцарским ученым-исследователем Philippe Oechslin метод получил название «Time-Memory Trade-Off» (компромисс между временем и памятью) [23]. Для проверки теоретических положений была разработана программа RainbowCrack [24].

Программа позволяет построить предварительные хэш-таблицы для заданного набора символов и далее по готовым таблицам подбирать пароли. Например, для подбора паролей состоящих только из символов латинского алфавита и длиной не более 7 символов, зашифрованных с помощью алгоритма, применяемого в LAN Manager, потребуется не более 3-х суток вычислений на компьютере Celeron 666 MHz. Объем таблиц составит порядка 610 Мбайт. Далее, с имеющейся таблицей подбор любого пароля, удовлетворяющего заданным условиям, составит не более 10 секунд. Существуют и онлайновые подборщики паролей, однако они ограничены по длине подбираемых паролей.

Автор приводит и другие расчеты. Например, создание таблицы для подбора паролей, состоящих из всех символов латинского алфавита, цифр и специальных символов и длиной не более 7 символов, потребует около 7, 5 лет вычислений на Celeron 666 MHz при общем объеме базы 119 Gb. Конечно, использование параллельных вычислений и более мощных вычислительных станций может значительно сократить время создания подобных таблиц.

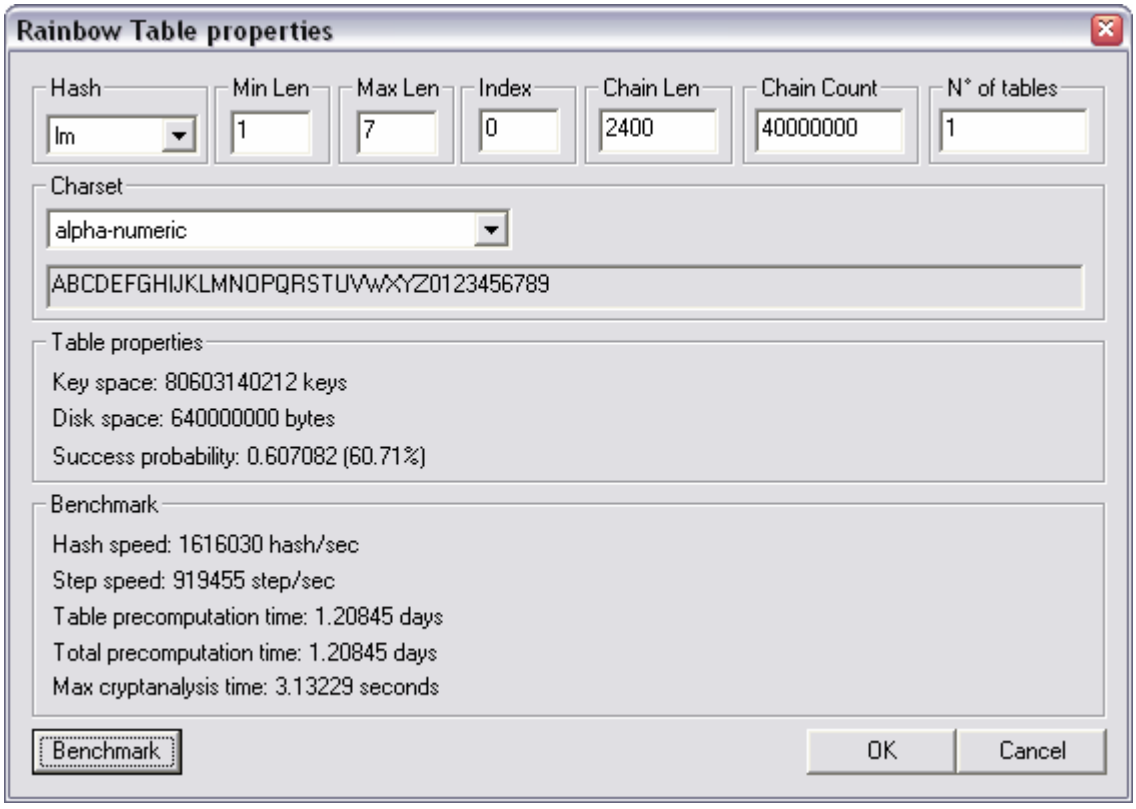

Рисунок 33. Окно программы Winrtgen 1.1 для генерирования хэш-таблиц.

Активные методы воздействия

Сканеры уязвимостей

Сканирование уязвимостей – это автоматизированный процесс, направленный на обнаружение известных уязвимостей в сетевых и программных платформах. Администраторы используют сканеры уязвимостей для оценки эффективности защиты компонентов их корпоративной сети. В результате анализа определяются уязвимые места системы, которые могут быть использованы злоумышленниками для осуществления несанкционированного доступа, и администратор принимает меры по их устранению. Таким образом, результатом работы сканера является достаточно подробная информация о корпоративной сети, включающая список сетевого оборудования, компьютеров, с запущенными на них службами, версиями сетевого программного обеспечения, уязвимостей присущих данному ПО, учетные записи пользователей системы.

Таким образом, сканирование злоумышленником уязвимостей является этапом, предваряющим атаку. На практике, внутренний нарушитель может собрать очень важную информацию, которая является недоступной для него в рамках служебных полномочий. Например, определить роли компьютеров в корпоративной сети, выделить файловые сервера и сервера баз данных, маршрутизаторы и интеллектуальные коммутаторы. И что особенно важно, именно результаты сканирования позволяют точно подобрать эксплойты для осуществления непосредственно несанкционированного доступа к узлам корпоративной сети. Рассмотрим результаты использование сканера уязвимостей Internet Security Scanner (ISS) в моделируемой корпоративной сети (рис 34.). Следует отметить, что злоумышленник для этих целей, вероятнее всего, воспользуется одним из бесплатных сканеров. Однако применение в данном примере коммерческого сканера ISS обусловлено тем, что это один из лучших инструментов для анализа защищенности сетей.

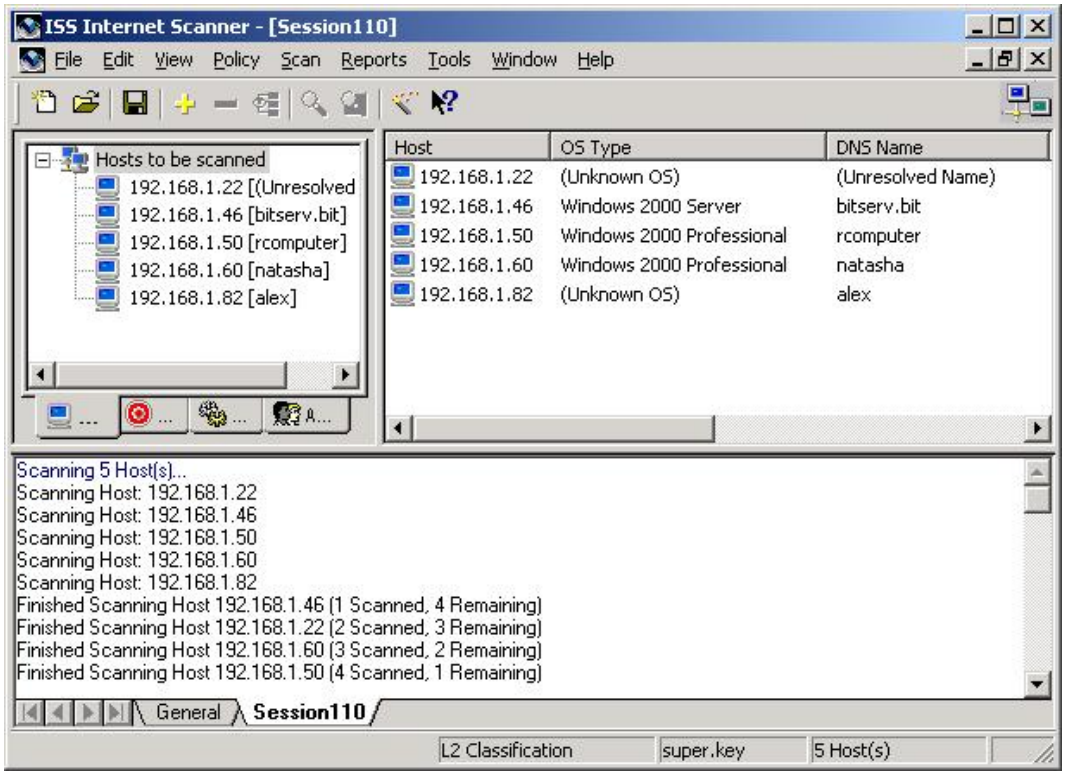

Рисунок 34. Результаты сканирования типовой сети

Злоумышленник, проанализировав службы, запущенные на хостах, может разделить их по функциональному признаку – доменные контроллеры, файловые, терминальные, принт-сервера, рабочие станции. По результатам сканирования можно выяснить, каким известным уязвимостям подвержены исследуемые хосты, и подобрать для последующей атаки соответствующие эксплойты.

Сетевые атаки

Все сетевые атаки по способу манипуляции с данными можно разделить на три группы:

- атаки, основанные на переполнении буфера (overflow based attacks)
- атаки, направленные на отказ-в-обслуживании (Denial-Of-Service attacks)
- другие атаки

Атаки, основанные на переполнении буфера, используют уязвимость системы, заключающуюся в некорректной программной обработке данных. При этом появляется возможность выполнения вредоносного кода с повышенными привилегиями.

Рассмотрим реализацию атаки подобного типа на примере уязвимости, найденной в Microsoft Internet Information Services (IIS) 4.0 и 5.0. Уязвимость позволяет злоумышленнику выполнить удаленное переполнение буфера. Некорректную проверку границ переменных производит ISAPI фильтр при обработке параметров .IDA файлов. Сетевой червь Code Red использует данную уязвимость для проникновения на веб-сервер, используя следующий запрос:

http://www.example.com/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u90
90%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090
%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a

В данном примере, 224 символа N в качестве аргумента передаются файлу default.ida и используются для переполнения буфера. Следующий далее машинный код внедряется (inject) в стек и исполняется на атакуемом сервере.

Атаки типа отказ-в-обслуживании не обязательно используют уязвимости в программном обеспечении атакуемой системы. Нарушение работоспособности системы происходит из-за того, что посылаемые ей данные приводят к значительному расходу ресурсов системы.

Самым простым примером атаки этого типа является атака «Ping Of Death». Сущность его в следующем: на машину жертвы посылается сильно фрагментированный ICMP пакет большого размера (64KB). Реакцией систем Windows 95/98 на получение такого пакета является полное зависание.

Другие виды атак используют ошибки в конфигурации сетевых сервисов, позволяющие злоумышленникам выполнять системные команды и получать несанкционированный доступ к данным. Примером здесь могут быть атаки, использующие размещенные на веб-сервере уязвимые CGI-скрипты. Задавая специальные параметры этим скриптам, злоумышленник может получить, например, доступ к файловой системе веб-сервера.

Рассмотрим более подробно сетевые атаки, основанные на использовании уязвимостей в программном обеспечении сетевых приложений.

Перевода термина "exploit" в отечественных публикациях не встречается, и эквивалента этого слова в русском языке также нет.

Поэтому в дальнейшем будет использоваться транслитерация с английского – "эксплойт". Данный класс атак основан на эксплуатации различных дефектов в программном обеспечении (потому и получил такое название – от англ. эксплуатировать, использовать). Следует отметить, что в последнее время наряду с термином «exploit», стал применяться термин «PoC» (от англ. Proof of Concept – дословно доказательство идеи, решения или демонстрационный пример). Данный термин более точно отражает исследовательский смысл эксплойта – демонстрация, подтверждающая возможность реализации найденной уязвимости. Потому на сайтах, посвященных информационной безопасности, чаще используется именно термин PoC.

Эксплойты представляют собой вредоносные программы, реализующие известную уязвимость в ОС или прикладном ПО, для получения несанкционированного доступа к уязвимому хосту или нарушение его работоспособности. Современные программные продукты из-за конкуренции попадают в продажу с ошибками и недоработками. Разработчики, включая в свои изделия всевозможные функции, не успевают выполнить качественную отладку создаваемых программных систем. Ошибки и недоработки, оставшиеся в этих системах, приводят к случайным и преднамеренным нарушениям информационной безопасности. Например, причинами большинства случайных потерь информации являются отказы в работе программно-аппаратных средств, а большинство атак на компьютерные системы основаны на найденных ошибках и недоработках в программном обеспечении. Так, например, за первые полгода после выпуска серверной операционной системы компании Microsoft Windows Server 2003 было обнаружено 14 уязвимостей, 6 из которых являются критически важными [25]. Несмотря на то, что со временем Microsoft разрабатывает пакеты обновления, устраняющие обнаруженные недоработки, пользователи уже успевают пострадать от нарушений информационной безопасности, случившихся по причине оставшихся ошибок. Такая же ситуация имеет место и с программными продуктами других фирм.

Таким образом, перед администраторами стоит проблема слежения за периодическим установлением обновлений и заплаток ПО, устраняющих известные уязвимости. Однако, как показывает практика, обновления устанавливаются крайне нерегулярно. Более того, после установки некоторых заплаток, вносящих изменения в ОС, некоторое прикладное ПО перестает нормально функционировать. Администраторы бывают вынуждены отказаться от установки обновлений, чтобы сохранить работоспособность корпоративного ПО. Такая ситуация создает дополнительные угрозы.

Рассмотрим действие эксплойтов на примере эксплойта KaHt2, реализующего одну из самых серьезных уязвимостей, найденную в MS Windows. Данный эксплойт организовывает атаку типа «отказ-в-обслуживании» (Denial-Of-Service, DoS) на службу «Удаленного вызова процедур» (Remote Procedure Call, RPC). Атаке уязвимы системы MS Windows NT/2000/XP/2003 [18]. Эксплойт KaHt2, реализует атаку на службу RPC, в результате которой осуществляется ошибка переполнения буфера, позволяющая злоумышленнику выполнить любой код на удаленной системе (рис. 35).

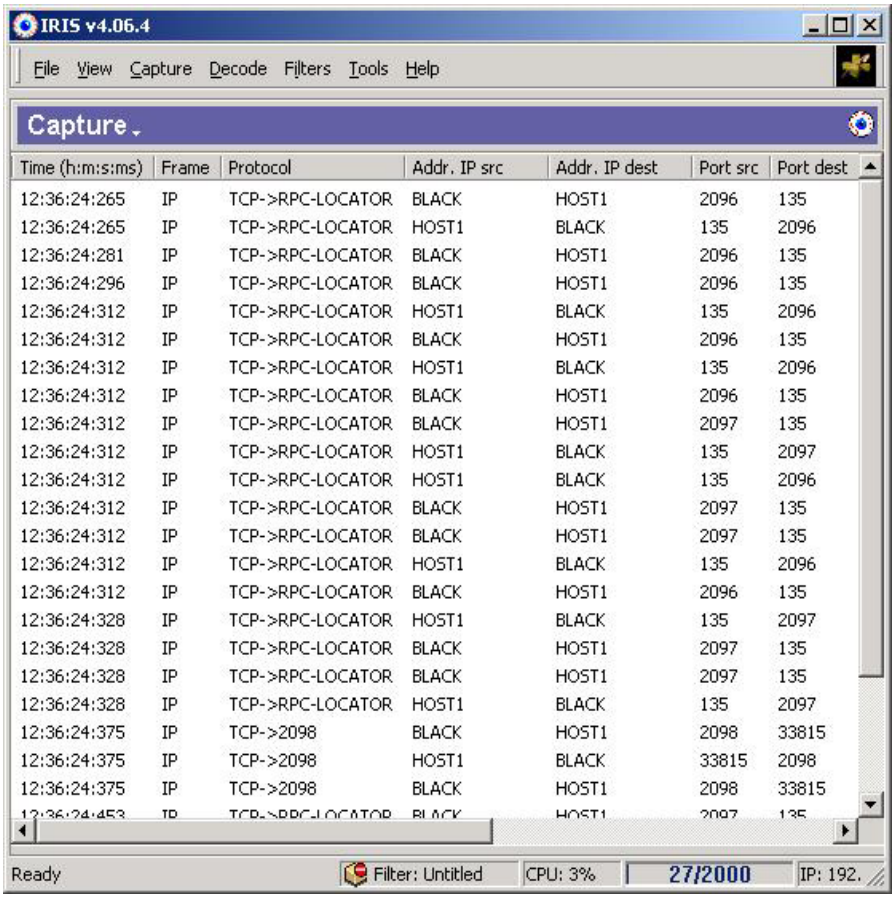

Рисунок 35. Атака на службу RPC (135-й порт) с хоста BLACK на хост HOST1

В процессе атаки в течение короткого промежутка времени (порядка 0,1 сек.) на 135-й порт, отвечающий за службу RPC, с хоста злоумышленника BLACK посылается шторм TCP-пакетов на хост HOST1. В силу уязвимости службы RPC на узле HOST1 возникает ошибка переполнения буфера и выполняется код эксплойта, открывающий командную оболочку на порте 33815.

Действие всех эксплойтов сводится либо к получению удаленного доступа к атакуемой системе в виде командной оболочки, т.н. шелла (shell или rootshell), либо в удаленном выполнении какой-либо

системной команды (например, добавление нового пользователя командой *net user add*), либо к вынужденной перезагрузке удаленной системы (рис. 36).

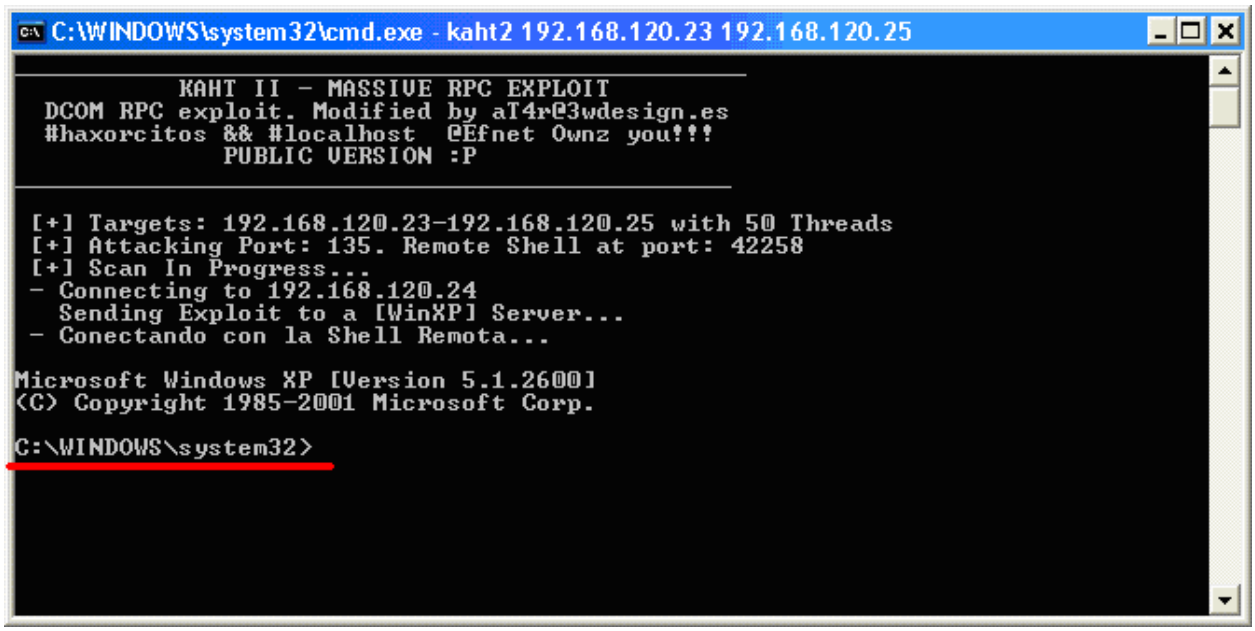

Рисунок 36. В результате реализации уязвимости Windows XP SP1 эксплойтом kaHt2 получена командная оболочка удаленной системы.

Для данного и многих других эксплойтов характерно наличие функций подавления антивирусных программ и межсетевых экранов.

Последствия применения эксплойтов могут быть самыми критическими. В случае получения злоумышленником удаленного доступа к системе, он имеет практически полный (системный) доступ к компьютеру. Последующие действия злоумышленника и ущерб от них могут быть следующими:

- внедрение троянской программы. Блокируя работу антивируса, можно установить на скомпрометированной системе программу удаленного администрирования – так называемого троянского коня. Последствия использования данных программ будет рассмотрено в следующем параграфе;
- внедрение набора утилит для сокрытия факта компрометации системы, так называемых Rootkits;
- несанкционированное копирование злоумышленником данных с жестким и съемных носителей информации скомпрометированной системы;

- заведение на удаленном компьютере новых учетных записей с любыми правами в системе для последующего доступа как удаленно, так и локально;
- кража файла с хэшами паролей пользователей компьютера для их последующего подбора. В случае если скомпрометированной системой является доменный контроллер, то под угрозой оказываются все пользователи данного домена.
- уничтожение или модификация информации на удаленном хосте. Может привести к значительным финансовым или материальным потерям.
- осуществление действий от имени пользователя скомпрометированной системы.

Троянские программы

Троянские программы (Trojans) – вредоносные программы, основное предназначение которых незаметно проникнуть на компьютер под видом законной программы и выполнить вредоносные действия. Троянские программы (также называемые троянцами или троянскими конями) состоят из двух частей: серверной (server) и клиентской (client). Когда пользователь, не подозревая, запускает серверную часть троянской программы, злоумышленник использует клиентскую часть для соединения с сервером по сети. Соединение обычно устанавливается по протоколам TCP и UDP. Будучи запущенной, серверная часть предпринимает действия, направленные на сокрытие своего присутствия в системе, маскируясь под другие процессы (рис.), ожидает соединения клиентской части на определенном порту, пытаются остановить работу антивирусов и межсетевых экранов, препятствующих его функционированию. Также, сервер троянской программы обеспечивает свой запуск при следующей загрузке системы – в Windows для этого есть несколько способов. Для использования серверной части троянской программы, злоумышленнику необходимо знать IP-адрес скомпрометированной системы. Поскольку даже внутри корпоративной сети возможно применение динамической адресации (DHCP), когда при каждой загрузке хост получает новый IP-адрес, троянские программы имеют средства оповещения злоумышленника об IP-адресе зараженной системы. Так возможна отправка серверной

частью адреса компьютера-жертвы на электронный адрес, по ICQ или IRC.

Обычно троянские программы выполняют одну или несколько задач:

- предоставление удаленного доступа злоумышленнику (remote access). Наиболее распространенная функция троянских программ, позволяющая злоумышленнику получить полный доступ к компьютеру-жертве.
- перехват и пересылка паролей. Троянские программы часто крадут пароли для популярных программ, таких как Outlook, ICQ и т.д. из кэша или конфигурационных файлов, а также путем отслеживания нажатий клавиш. Собранные пароли отсылаются на электронный адрес.
- запись всех нажатий клавиатурных клавиш (keyloggers). В данном случае в файл записываются все подряд нажатия клавиш, для последующего анализа нужной информации. Файл с данными также пересылается по электронной почте.
- уничтожение файлов. Троянские программы с такой деструктивной функцией также известны как логические бомбы. Чаще всего они удаляют определенные файлы на компьютере-жертве в заданное время.
- создание платформы для распределенной DoS-атаки. Использование троянских программ позволяет подготовить платформу – агентов для проведения распределенных DoS-атак. Злоумышленник, управляя агентами, в определенный период времени со множества компьютеров-жертв одновременно осуществляется атака на определенный узел сети.

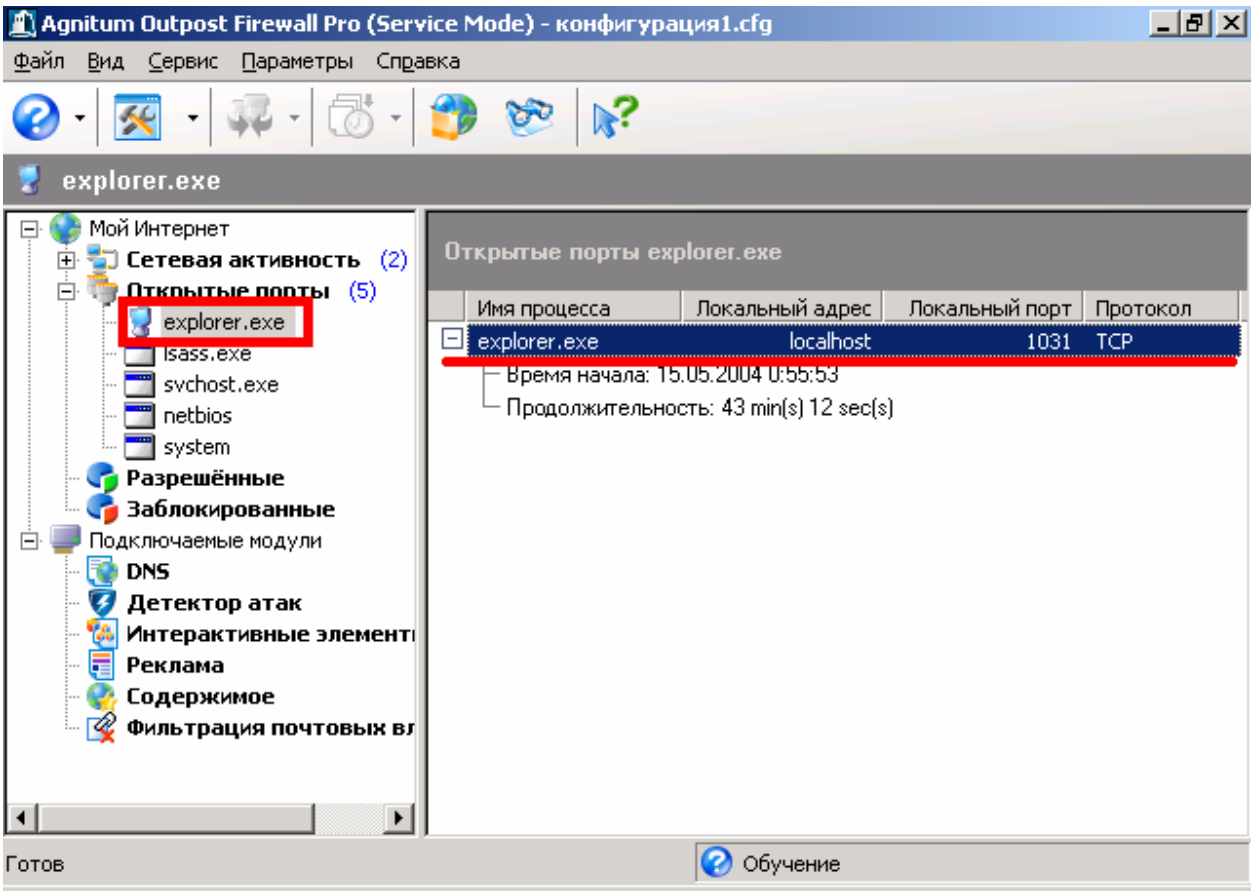

Рис 37 . Троянская программа Back Orifice 2000 ожидает соединения на 1031 порту и маскируется в списке процессов под приложение Windows Explorer.

Ущерб, наносимый троянскими программами, может быть очень велик – кража паролей, конфиденциальной информации, удаление, блокирование или модификация информации на скомпрометированном компьютере посредством удаленного управления.

Основными способами проникновения троянских программ в настоящее время являются:

- Запуск вложений в письмах электронной почты;
- Запуск активного содержимого web-страниц неблагонадежных web-сайтов;
- Запуск непроверенных антивирусным ПО программ из внешних источников.

Утилиты для сокрытия факта компрометации системы (Rootkits)

Существуют специально разработанные утилиты для сокрытия факта компрометации системы, путем скрытия всех фактов деятельности злоумышленника. Такие утилиты есть для различных систем и Windows, и Linux, и называются Rootkits, что можно перевести как набор административных утилит.

В частности, утилита AFX Windows Rootkit 2003 из данного класса программ позволяет сконфигурировать специальный патч (заплатку), установка которого в ОС Windows 9x/NT/2000/XP/2003 скрывает указанные процессы, файлы, каталоги, ключи реестра, а также сетевую активность. Таким образом, администратор скомпрометированной системы не увидит в списке процессов никаких подозрительных программ, и никаких подозрительных сетевых соединений, выдаваемых, к примеру, командой netstat.

Демонстрационное использование данной утилиты для сокрытия определенного процесса представлено на рисунках 38-39.

Рисунок 38. Генерирование патча с использованием AFX Windows Rootkit 2003 для сокрытия всех процессов, в названии которых есть слово notepad.

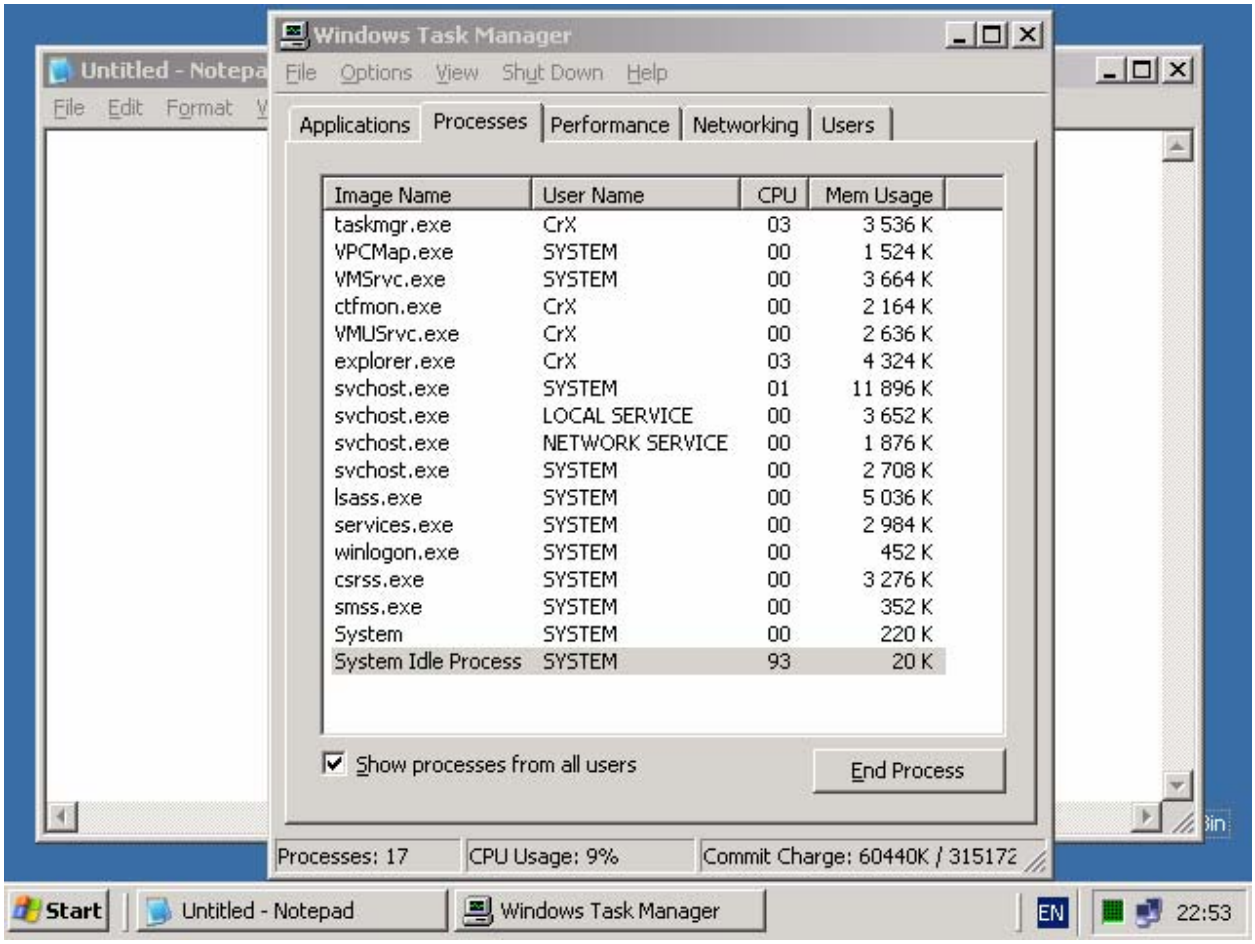

Рисунок 39. Запущен текстовый редактор Notepad, однако в окне процессов Task Manager, соответствующий процесс не отображается.

Вирусы и сетевые черви

Вирусы могут быть серьезным орудием в руках внутреннего нарушителя. Применение вирусов и сетевых червей позволяет достигнуть следующих целей:

- Уничтожение или непоправимое изменение текстовых документов, исполняемых файлов, баз данных;
- Нарушение работоспособности всей корпоративной сети и отдельных элементов: серверов, рабочих станций.

Потери от вирусной эпидемии для компании могут быть непоправимыми. Так, существуют специализированные версии вирусов-червей, например, червя MyDoom, уничтожающего только все офисные документы – форматов Word, Excel, Access и т.д. Учитывая, что 70-90% интеллектуального капитала современной компании хранится в электронном виде, серьезная вирусная атака может нанести значительный ущерб. Финансовые потери от простаивания и затраты на восстановление также могут быть весомыми (рисунок 40).

Последствие	Процент (%)
Потеря производительности	75
Компьютеры были недоступны	69
Повреждения файлов	62
Потеря доступа к файлам	49
Потеря данных	47
Потеря доверия пользователей	33
Закрытие доступа	18
Ненадежность прикладного ПО	13
Трудности с чтением файлов	12
Трудности с сохранением файлов	9
Падение системы	9
Трудности с выводом на печать	7
Угроза потерять работу	2

Рисунок 40. Последствия для компаний от вирусных атак.

Способы проникновения вирусов в корпоративную сеть аналогичны описанным выше для троянских программ. В последние годы появился новый источник проникновения сетевых червей – через IM-клиентов. Только в 2002 году появилось 5 известных IM-червей, а уже в начале 2004 года по данным Лаборатории Касперского в мире прошла первая глобальная эпидемия нового сетевого червя «Bizex» среди пользователей интернет-пейджера ICQ. Механизм распространения IM-червей рассмотрим на примере червя «Bizex». На компьютер жертвы доставляется ICQ-сообщение, где, в частности, предлагается посетить некий веб-сайт. Для маскировки пользователю показываются мультфильмы из популярного сериала "Joecartoon". Тем временем в систему незаметно проникает Java-вирус, который, используя брешь в ICQ, незаметно рассылает от имени владельца компьютера ссылку на вышеуказанный веб-сайт по всем получателям из контактного листа. Избежать заражения можно, немедленно удалив данное сообщение и не посещая указанный сайт. Отметим, что ни один из видов современных IM-червей пока еще не способен автоматически выполнятся после

получения. Поэтому, если пользователи IM-систем в компании лучше узнают обо всех имеющихся угрозах и методах их предотвращения, способность червей к размножению будет существенно снижена.

Источники вирусов	1996 г.	1997 г.	1998 г.	1999 г.	2000 г.	2001 г.	2002 г.
Приложения к электронным письмам	9	26	32	56	87	83	86
Файлы, загружаемые через Интернет	10	16	9	11	1	13	11
Через просмотр веб-сайтов	0	5	2	3	0	7	4
Другие пути	0	5	1	1	1	2	3
Дискеты	71	84	64	27	7	1	0

Рисунок 41. Способы проникновения вирусов в компьютеры, %

Несанкционированная установка дополнительных технических средств

Угроза несанкционированной установки дополнительных технических средств заключается в установке нарушителем специализированных технических средств, облегчающих осуществление НСД. Например, инсталляция модема на рабочем месте пользователя и подключение его к телефонному проводу позволит последнему осуществлять неконтролируемый доступ к корпоративной сети извне. Данная угроза очень опасна так, как появляется «черный ход» в корпоративную сеть в обход средств защиты установленных для препятствования внешним нарушителям. В то время, как установка модема внешнего или внутреннего все-таки операция, которую трудно

произвести скрытно, тем более в процессе передачи информации необходимо занять офисную телефонную линию, широкое распространение мобильных телефонов приводит к новой расстановке приоритетов угроз. В большинстве современных мобильных телефонов имеется встроенный модем, который можно использовать для подключения к Интернет. Скорость соединения варьируется от 1 Кб/с до нескольких десятков Кб/с (например, для технологии GPRS), что позволяет передавать по нему достаточно большие объемы информации. Чтобы использовать модем, встроенный в мобильный телефон, последний подключается к компьютеру либо в параллельный порт с помощью специализированного кабеля, либо по инфракрасной связи. Таким образом, если не принято специальных мер, любой сотрудник может принести современный мобильный телефон и, подключив его к своей рабочей станции, скрытно передать из организации доступные ему материалы, практически любого объема. Возможно также, через оставленный на ночь в режиме модема телефон, осуществить удаленную атаку на корпоративную сеть. Причем в этом случае работу по проникновению может провести уже не внутренний сотрудник, а высококвалифицированный злоумышленник, так называемый «хакер». В таком случае перед ним будет открыта корпоративная сеть, значительно меньше защищенная, чем от нападения снаружи. Ущерб от реализации такой угрозы может быть очень велик.

Защита корпоративных сетей от внутренних злоумышленников.

Противодействие пассивным методам воздействия

Противодействие угрозе прослушивания сетевого трафика

Как показано выше, данная угроза осуществима в сетях, построенных как на концентраторах, так и на коммутаторах. Однако в каждом случае реализация угрозы имеет свои особенности.

Для прослушивания сетевого трафика в сети, построенной на концентраторах злоумышленнику достаточно запустить на своем компьютере программу-снифер и анализировать проходящие пакеты. Поскольку данная атака носит пассивный характер (нет непосредственного воздействия), то обнаружить ее достаточно тяжело. Теоретически это даже невозможно, поскольку снифферы только

собирают пакеты, и не передают никакой информации. Однако на практике в ряде случаев это возможно. Рассмотрим некоторые существующие методы определения наличия запущенного сниффера в локальной сети – это метод пинга, метод ARP, метод DNS и метод ловушки [19].

Метод пинга (Ping method) использует уловку, заключающуюся в отсылке «ICMP Echo request» (Ping запроса) не на MAC-адрес машины, а на ее IP-адрес. Проиллюстрируем использование данного метода на примере.

1. Допустим, хост, который мы подозреваем на использование сниффера, имеет IP-адрес 10.1.1.1 и MAC-адрес 00-40-05-A4-79-3**2**.
2. Ваш компьютер должен находиться в том же сегменте ЛВС, что и подозреваемый компьютер.
3. Вы посылаете «ICMP Echo request», указав в запросе IP-адрес подозреваемого хоста и его слегка измененный MAC-адрес, например, 00-40-05-A4-79-3**3**.
4. Каждый хост, получив данный запрос, сравнивает указанный в запросе MAC-адрес со своим MAC-адресом. В случае совпадения MAC-адресов, хост отвечает источнику запроса с помощью «ICMP Echo Reply», иначе пакет игнорируется. В данном случае, ни один из хостов в ЛВС не должен увидеть данный пакет.
5. Если же получен ответ от какого-либо хоста, это значит что у него не используется фильтр MAC-адресов, т.е. его сетевой адаптер находится в «беспорядочном режиме». Следовательно на данном хосте используется сниффер.

Метод пинга может быть перенесен на другие протоколы, которые генерируют ответы на запросы, например, запрос на установление TCP-соединения или запрос по протоколу UDP на порт 7 (эхо).

Метод ARP (ARP method) использует похожую технику, а также особенности реализации протокола ARP в Windows и Linux. Рассмотрим действие данного метода на примере определения хоста под управлением Windows с запущенным сниффером.

1. Вы подозреваете, что на хосте (A) с IP-адресом 192.168.86.19 запущен сниффер. Если вы разошлете широковещательный ARP-запрос, которому соответствует Ethernet-адрес «FF:FF:FF:FF:FF:FF», с целью выяснения MAC-адреса хоста (A), все хосты должны получить ваш запрос, но ответит только тот, чей IP-адрес указан в ARP-запросе (т.е. подозреваемый). В таблице приведены поля пакета рассылаемого ARP-запроса.

Ethernet-адрес хоста-получателя	FF:FF:FF:FF:FF:FF
Ethernet-адрес хоста-отправителя	Собственный MAC-

	адрес
Тип протокола (ARP=0806)	08 06
Адресное пространство (Ethernet=01)	00 01
…	
Аппаратный адрес хоста-отправителя	Собственный MAC-адрес
IP-адрес хоста-отправителя	Собственный IP-адрес
Аппаратный адрес хоста-получателя	00 00 00 00 00 00
IP-адрес хоста-получателя	IP-адрес хоста (A)

А на рисунке 42 приведен сам ARP-запрос в окне детализации анализатора протоколов Sniffer Pro.

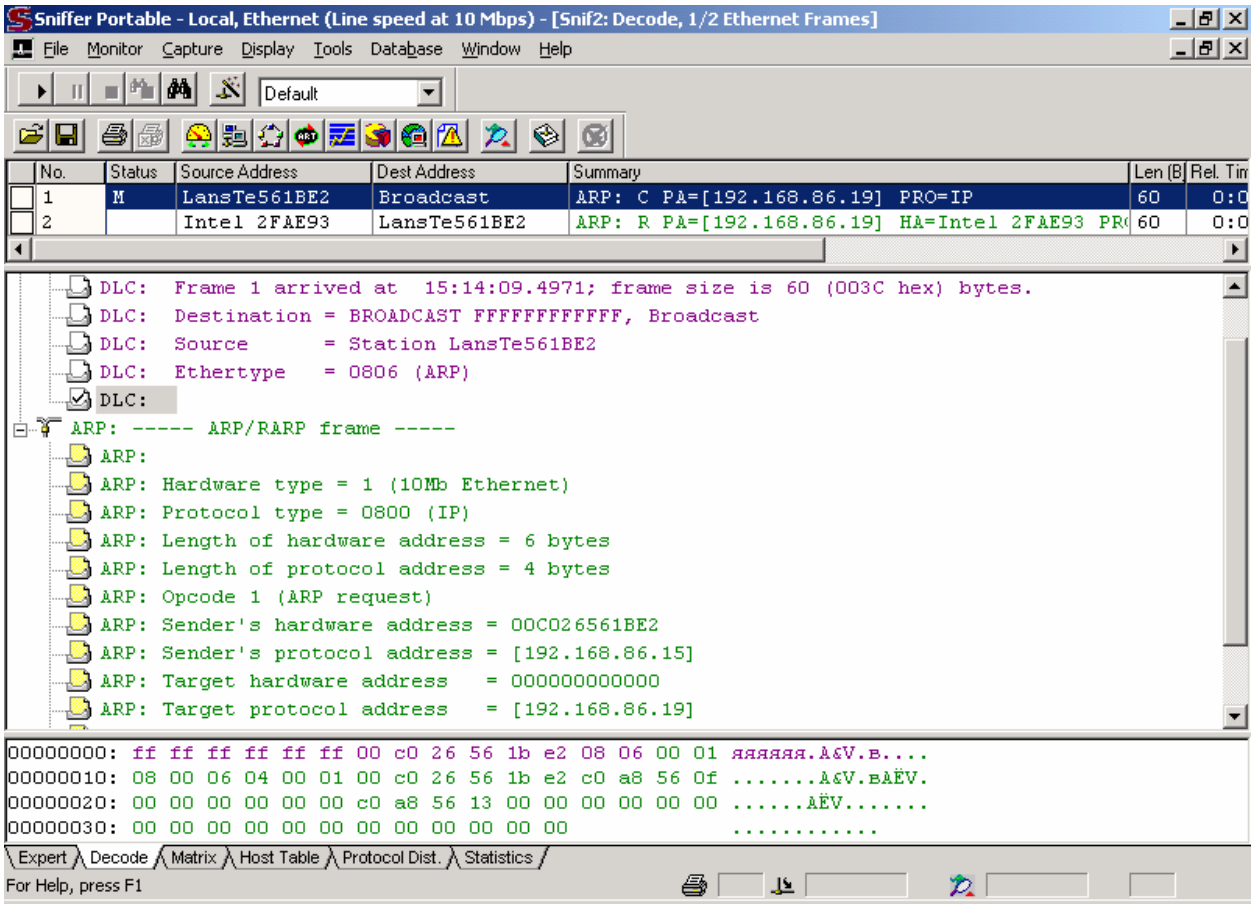

Рисунок 42. Широковещательный ARP-запрос в окне анализатора протоколов Sniffer Pro для выяснения MAC-адреса хоста с IP-адресом 192.168.86.19.

Однако было обнаружено, что если на хосте запущен сниффер, то в некоторых случаях он неправильно обрабатывает ARP-запросы.

2. Используя предложенный метод, вы посылаете точно такой же ARP-запрос, но где вместо широковещательного адреса «FF:FF:FF:FF:FF:FF» указан адрес «FF:FF:FF:FF:FF:FE» (ложный широковещательный адрес, из которого вычли один бит). Поскольку адрес не является широковещательным, теоретически ни один из хостов не должен ответить на такой запрос. Однако практические эксперименты, что Windows 2000/XP/2003 при условии, что сетевой адаптер, работает в беспорядочном режиме, посчитает такой запрос широковещательным. Соответственно хост (A), на котором запущен сниффер, сравнив IP-адрес в запросе со своим IP-адресом, пошлет ответ ARP-reply. Таким образом, хост (A) выдаст, что он прослушивает весь сетевой трафик. Ситуацию иллюстрируют следующие экранные снимки, сделанные с анализатора протоколов Sniffer Pro:

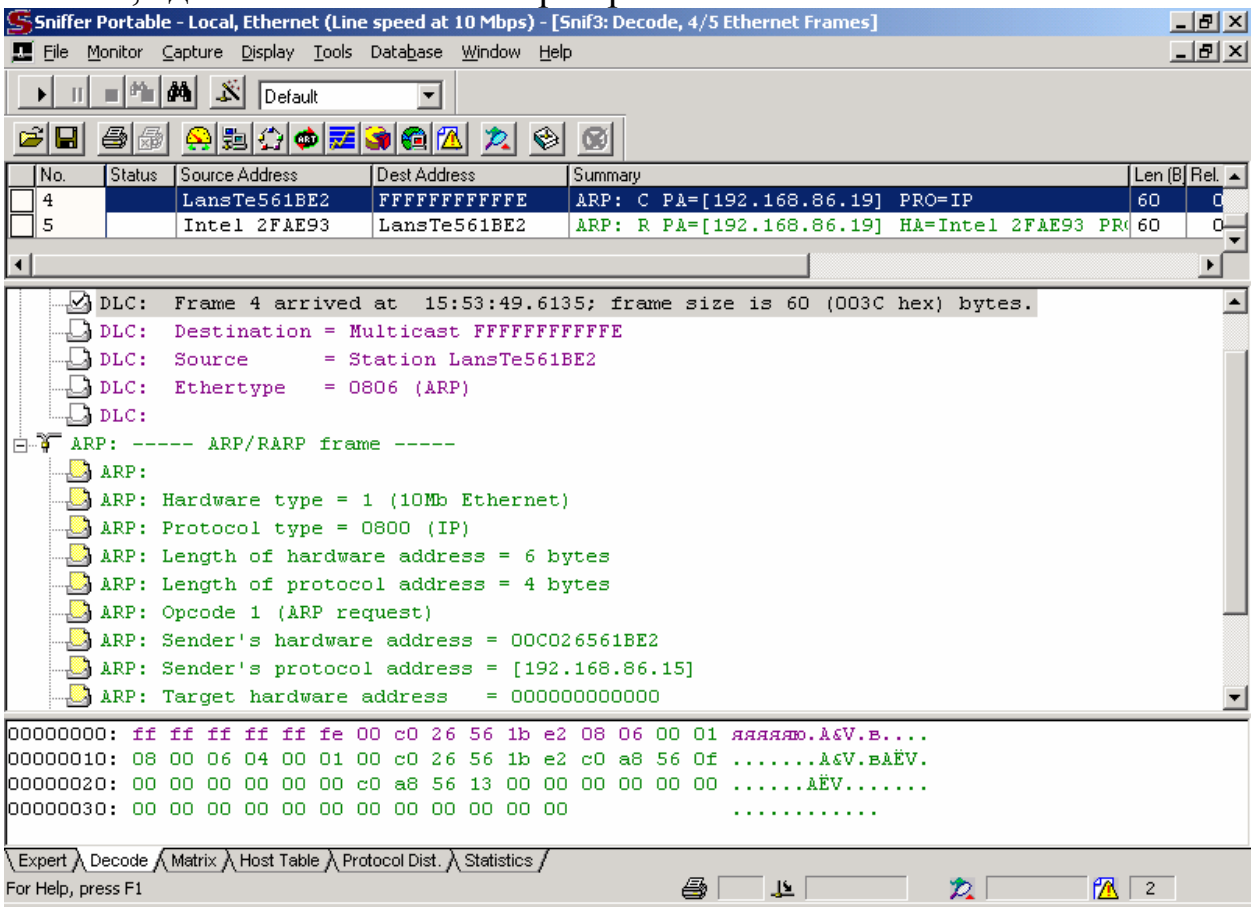

Рисунок 43. Рассылка ARP-запроса на ложный широковещательный адрес «FF:FF:FF:FF:FF:FE».

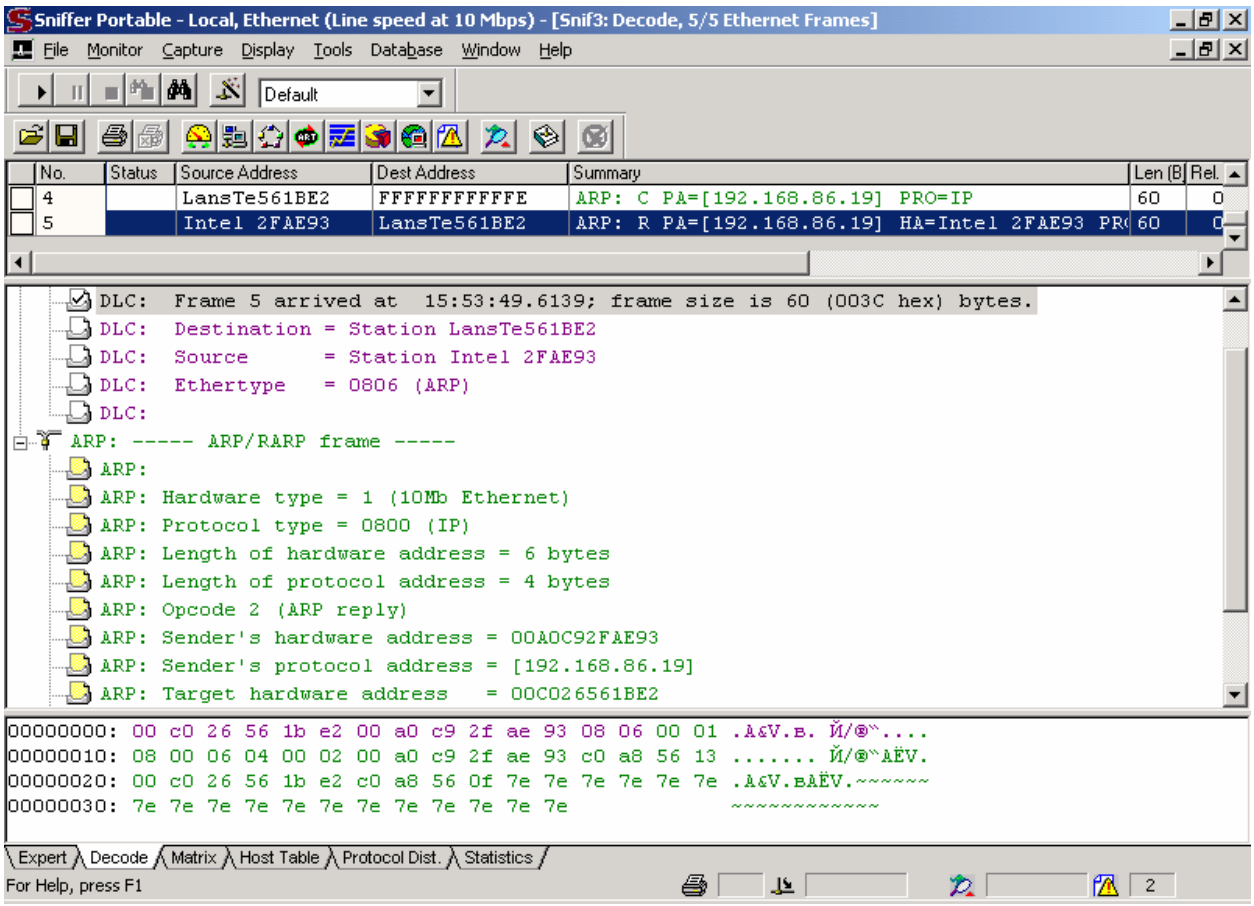

Рисунок 44. Хост (A) отвечает ARP-ответом на ложный широковещательный ARP-запрос, выдавая тем самым, что на нем запущен сниффер.

Экспериментальным путем были созданы таблицы аномальных ответов на различные ARP-запросы для современных ОС – Windows 9x/2000/NT и Linux, в которых запущены снифферы.

Отметим только, что данные методы в большинстве случаев позволяют лишь с некоторой вероятностью определить наличие сниффера. В настоящее время существует множество бесплатных и коммерческих снифферов, которые можно найти в Интернет. А программ, удаленно определяющих их наличие, не так много. Рассмотрим наиболее популярные из таких программ: L0pth Antisniff, Cain&Abel и PMD:

- L0pht Antisniff реализует большинство известных методов обнаружения снифферов, однако данная программа написана в 1998 году, финальная версия так и не вышла (доступна только beta), и в настоящее производителем не поддерживается. Программа функционирует только под ОС Windows 9x/NT и не работает под Windows 2000/XP, что накладывает серьезные ограничения на ее использование.

- Cain&Abel, уже упоминавшаяся утилита, имеет реализацию средств определения снифферов на основе ARP-метода (рис 45).
- PMD (Promiscuous Mode Detector) из комплекта Anti Sniff Toolbox, разработанного Roberto Larcher. В программе используется метод ARP.

Эксперимент в тестовой корпоративной сети с запущенными снифферами – IRIS Network Analyzer, Sniffer Pro, TCP Dump, показал, что в целом все три программы успешно определяют снифферы, однако для правильной настройки программ необходимо иметь теоретические сведения о работе методов обнаружения снифферов.

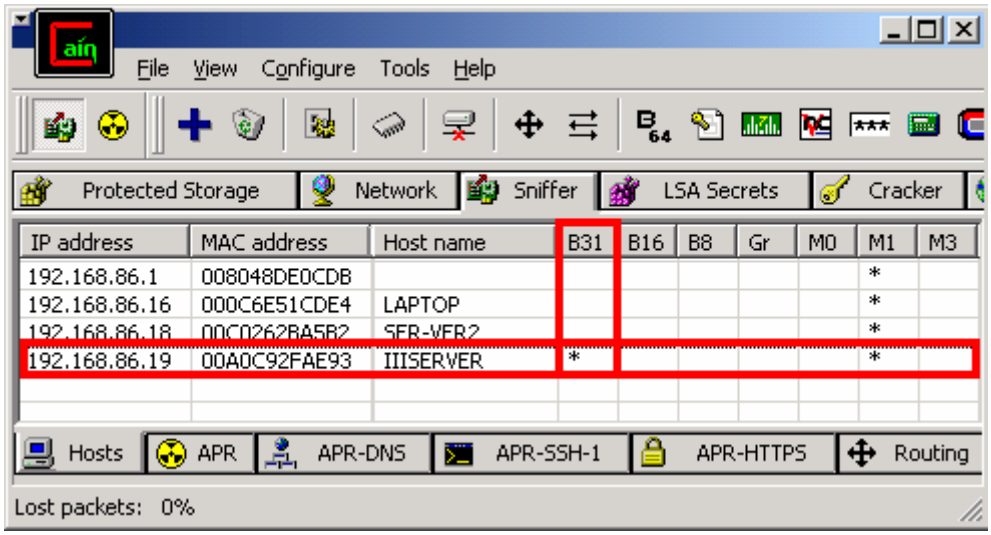

Рис 45. Определение сниффера на хосте с IP-адресом 192.168.86.19 с использованием рассылки ложного широковещательного ARP-запроса типа B31(«FF:FF:FF:FF:FF:FE»).

Для прослушивания сетевого трафика в сети, построенной на коммутаторах злоумышленнику необходимо реализовать одну из атак ARP-spoofing, MAC-duplicating или MAC-flooding. Поскольку все три атаки имеют активный характер, их теоретически можно обнаружить.

Реализацию атаки MAC-flooding выявить сравнительно легко – достаточно запустить на любом хосте сниффер и увидеть пакеты, не предназначенные данному хосту. Существуют и методы защиты от этой атаки. Многие современные коммутаторы поддерживают функцию «Port Security», назначение которой в жесткой фиксации MAC-адресов за портами коммутатора. Поскольку MAC-адреса уникальны, то подключение другого компьютера к порту коммутатора не позволит ему получить доступ к сетевым ресурсам. Данная мера эффективна против атак MAC-Flooding и MAC-Duplicating, однако не препятствует атаке ARP-Spoofing.

Современные межсетевые экраны и системы обнаружения вторжений в большинстве случаев не обнаруживают атаку ARP-spoofing. Конечно, это можно объяснить, тем, что уязвимость заложена в сам протокол ARP. Однако методы обнаружения атаки ARP-spoofing существуют и реализованы в некоторых специализированных программных средствах. Утилита ACiD (ARP Change Intrusion Detector) из комплекта Anti Sniff Toolbox, разработанного Roberto Larcher, выполняет мониторинга сетевого трафика с целью выявления аномалий, присущих атаке «отравления ARP-кэша» (рисунок 46).

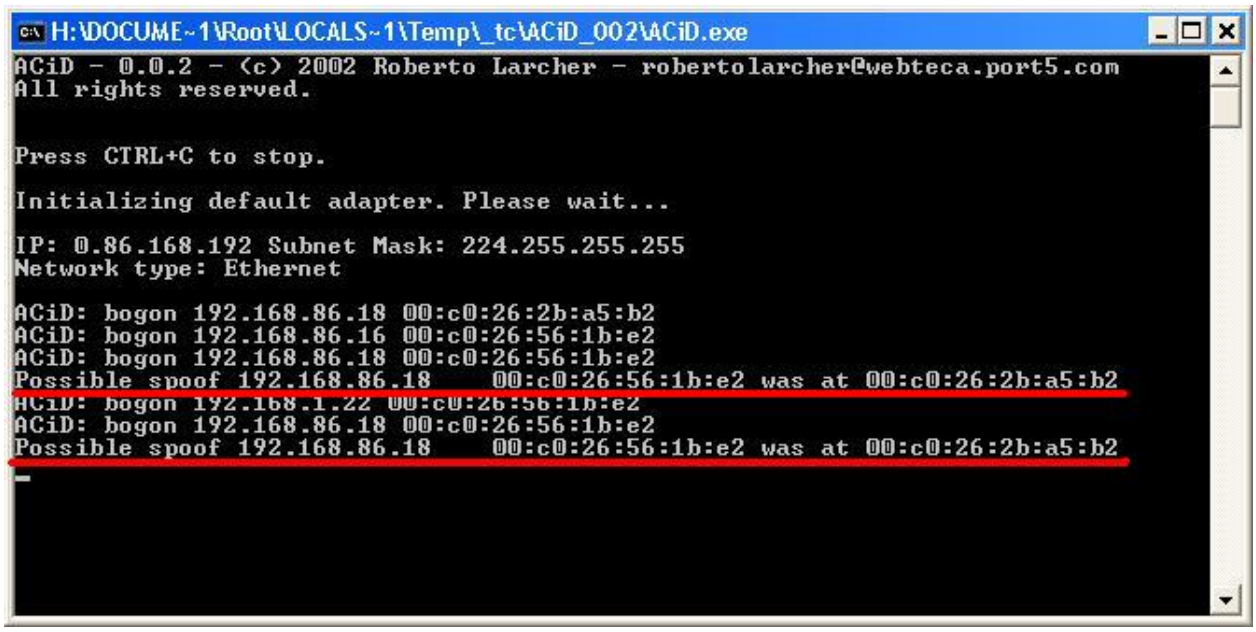

Рисунок 46. Определение атаки ARP-Spoofing программой ACiD.

Поскольку механизм атаки ARP-Spoofing основан на уязвимости в протоколе ARP, имеет смысл доработать данный протокол. Для ОС Linux есть утилита Arp_antidote, изменяющая реализацию протокола ARP в ОС таким образом, чтобы сделать данную атаку бессмысленной. Механизм обновленного протокола работает следующим образом. При приеме ARP-reply пакета производится сравнение старого и нового MAC-адреса, и при обнаружении его изменения запускается процедура верификации. Посылается ARP-запрос, требующий всем хозяевам IP-адреса сообщить свои MAC-адреса. В случае атаки ARP-Spoofing "настоящая" система, имеющая этот IP-адрес, ответит на запрос, и, таким образом, атака будет распознана. Если же изменение MAC-адреса было связано не с атакой, а со стандартными ситуациями, ответа, содержащего "старый" MAC-адрес, не будет, и по прошествии определенного таймаута система обновит запись в кэше. При

обнаружении подозрительной ситуации ("двойника") ядро выводит сообщение: "ARP_ANTIDOTE: Possible MITM attempt!" и не обновляет запись ARP-кэша, а наоборот, прописывает старую запись как статическую. О подобных утилитах или обновлениях для Windows неизвестно.

Использование статических ARP-записей не всегда является решением проблемы. Согласно исследованию на системах Windows 9x/NT/2000/XP/2003 статическая ARP запись может всегда быть перезаписана, используя фальшивое ARP сообщение.

Использование сетевых систем обнаружения вторжений, например ISS RealSecure, позволяет выявить ARP-атаку путем обнаружения в сети двух одинаковых IP-адресов.

Ну и, наконец, самым радикальным решением является сделать перехват сетевого трафика бессмысленным. Для этого необходимо применить механизмы шифрования. Замена всех небезопасных протоколов не всегда возможна. Более практичным является шифрование всего трафика на 3-м уровне модели OSI, используя протокол IPSec. При этом окажутся защищенными и все протоколы прикладного уровня – POP3, SMTP, FTP и т.д. Поддержка этого протокола в ОС семейства Windows реализована начиная с версии Windows 2000. Таким образом, клиенты с Windows NT4/9x/ME использовать данный протокол не могут. Однако существуют средства шифрования альтернативных разработчиков, в том числе сертифицированные Гостехкомиссией России. Их применение может поднять защиту сети на должный уровень.

Если применение протокола IPSec невозможно по каким-либо причинам, а поскольку как показано выше, раскрытие паролей корпоративной электронной почты может иметь серьезные последствия, необходимо предпринять меры по защите аутентификационных данных при доступе к почтовым серверам. Существуют специализированные протоколы защиты определенных протоколов прикладного уровня. Например, протоколы POP3S и SMTPS (POP3, SMTP over SSL) позволяет надежно зашифровать сообщения электронной почты. Подобные модификации есть и для протоколов HTTP – HTTPS, FTP – FTPS, IMAP – IMAPS и др., а их поддержка реализована во многих современных серверах и клиентах.

В случае применения защиты данных на сетевом уровне, защищенными также окажутся и аутентификационные данные пользователей к бесплатным электронным почтовым ящикам в Интернет. В противном случае, рекомендуется ограничить доступ пользователей корпоративной сети к бесплатным почтовым службам в Интернет.

Использование администратором специализированного сниффера, например уже упоминавшегося Cain, позволит увидеть сеть глазами потенциального нарушителя. А удобный интерфейс программы Cain позволит сразу же выявить слабые места в корпоративной сети. Например, сотруднику, воспользовавшемуся бесплатным почтовым ящиком в Интернет, можно продемонстрировать его пароль, перехваченный с помощью сниффера, и объяснить, что такое может сделать и внутренний нарушитель. Если же пароль к ящику совпадает с одним из корпоративных паролей, то это может скомпрометировать всю корпоративную сеть и сказаться на служебном положении работника. Такая организационные меры позволят снизить вероятность угроз, связанных с паролями. Следует отметить, что действия службы безопасности, направленные на скрытое наблюдение, могут трактоваться как вмешательство в частную жизнь. Однако во избежание подобной ситуации достаточно уведомить сотрудников с письменным подтверждением о прослушивании всех служб коммуникации установленных на рабочих местах.

Методы, снижающие риск угрозы расшифрования паролей

1. Всегда активизируйте опцию «Password must meet complexity requirements» («Пароли должны удовлетворять требованиям сложности») в политике безопасности Windows 2000/XP/2003. Данная функция предъявляет следующие требования к сложности паролей, назначаемых пользователю:

1.1. Пароль не может содержать какие-либо части пользовательского имени;

1.2. Длина пароля должна быть не менее 6 символов;

1.3. Пароль обязательно должен быть составлен из следующих символов:

- символы латинского алфавита в верхнем регистре;
- символы латинского алфавита в нижнем регистре;
- цифры от 0 до 9;
- специальные символы, например, !, $, #, %.

Примером пароля, удовлетворяющего указанным требованиям сложности, является пароль P@ssw0rd. Как показано выше, подбор паролей, созданных по такому принципу, гораздо сложнее как по методу перебора, так и по методу вычисления таблиц.

Используя Microsoft Platform Software Development Kit можно создавать специализированные фильтры паролей для особенных целей.

2. Минимальная длина пароля в Windows должна быть 15 символов. Как показано исследователям с сайта SecurityFriday.com для пароля длиной более 15 символов LM-хэш в Windows сохраняется некорректно, что не позволяет осуществлять подбор пароля по его хэшу. И хотя в Windows XP/2000/2003 пароли могут быть длиной до 127 символов, средства политики безопасности, позволяющие задать требование к минимальной длине пароля, ограничены 14 символами. То есть осуществить программный контроль за тем, чтобы пользователи задавали пароль не менее 15 символов средствами Windows нельзя. Однако сетевые администраторы и персонал службы безопасности должен обязательно следовать данной рекомендации.

Для облегчения запоминания паролей такой длины рекомендуется использовать в качестве пароля наборы слов или фразы, разделенные пробелами и дополненные цифрами и спец. символами.

3. Рекомендуется периодически менять пароли. Причем, периодичность должна варьироваться для разных групп пользователей. Частая смена паролей, особенно к которым предъявлены требования повышенной сложности и большой длины, приведет к росту недовольства пользователей и к придумыванию ими различных схем упрощения данной процедуры. Например, пароли будут записываться на бумажки и прятаться в «надежных» местах, или будет придумана предсказуемая схема создания нового пароля из старого и т.д. Поэтому периодичность смены паролей рекомендуется устанавливать в 3-6 месяцев.

4. Обучение пользователей надежно хранить пароли. Это конечно организационная мера, а не техническая, однако важность ее в данном разделе безусловна. Действительно, даже самый сложный и длинный пароль легко скомпрометировать, если пользователь хранит его в легкодоступном месте. Особенно в контексте противодействия внутренним нарушителям, которые могут скрытно выяснить места хранения паролей своими коллегами. Поэтому задача администратора сети или службы безопасности объяснить пользователям, что пароли рекомендуется хранить в надежных местах, например, сейфе или запираемом на ключ ящике. Пароли, записанные на бумажных носителях, необходимо не просто выкидывать, а уничтожать.

Иная ситуация для паролей на сервера и сетевое оборудование: маршрутизаторы, управляемые коммутаторы, МЭ и т.д. В этом случае пароли требуется документировать, поскольку их знание может потребоваться в случае болезни, увольнения, отсутствия лиц,

ответственных за оборудование. К журналу со списком паролей должны предъявляться повышенные требования организационного, технического и физического уровня обеспечения безопасного хранения.

Следует отметить распространенность программных средств, предлагающих хранить все пароли в одном защищенном криптографическими средствами программном файле. Такой способ имеет очевидный недостаток – при компрометации мастер-пароля на доступ к файлу со списком паролей, все пароли окажутся скомпрометированными.

Противодействие активным методам воздействия

Противодействовать активным воздействиям злоумышленников, как внутренних, так и внешних, призваны межсетевые экраны и системы обнаружения атак. Поскольку применение МЭ и СОА в данной главе рассматривается в контексте противодействия внутренним нарушителям, рассмотрены персональные МЭ и СОА уровня сети и хоста.

Обнаружение сканирования

Само по себе сканирование не является чем-то незаконным. С мнениями отечественных экспертов по данному вопросу можно ознакомиться здесь [26]. Однако, если сканирование со стороны внешней, по отношению к корпоративной, сети как показывает практика обыкновенное явление, то сканирование компьютеров из внутренней сети – безусловно, инцидент безопасности, требующий незамедлительной реакции со стороны сетевого администратора или администратора безопасности.

Обнаружить следы сканирования можно, изучая журналы регистрации МЭ. Однако такой подход не позволяет своевременно реагировать на подобные инциденты. Поэтому современные МЭ имеют модули (plug-in) позволяющие обнаружить атаки и сканирование в режиме реального времени, также как это сделано в СОА. Некоторые сканеры уязвимостей используют оригинальные методы, позволяющие производить сканирование максимально скрытно. Например, в одном из лучших сетевых сканеров Nmap существуют возможности, позволяющие значительно затруднить обнаружение сканирования для СОА:

- возможность задавать временные параметры сканирования – интервалы между пакетами. Для выявления такого сканирования необходимо проанализировать пакеты за значительный промежуток времени;
- возможность задавать группу ложных хостов, с которых якобы производится сканирования, для скрытия реального IP-адреса злоумышленника. Данная функция особенно опасна, т.к. в качестве ложных хостов могут быть указаны хосты легальных сотрудников, что значительно затруднит обнаружение настоящего нарушителя.

Решением против подобных методов сканирования может быть использование сетевых СОА, либо периодическое изучение журналов регистрации МЭ.

Противодействие эксплойтам

Как показали эксперименты, межсетевые экраны и системы обнаружения вторжений, установленные на атакуемой системе, в ряде случаев не в состоянии отразить действие эксплойтов. Для успешного отражения атак эксплойтов средства защиты необходимо обновлять, поскольку механизм обнаружения вторжений основан на распознавании сигнатур уже известных атак. Хотя существуют разработки, способные по заверениям разработчиков отражать неизвестные атаки, практика показывает, что они все еще не эффективны. На рисунке 47 проиллюстрировано как система обнаружения атак Black ICE 3.5 без установленных обновлений сигнатур атак не в состоянии отразить действие эксплойта KaHt2.

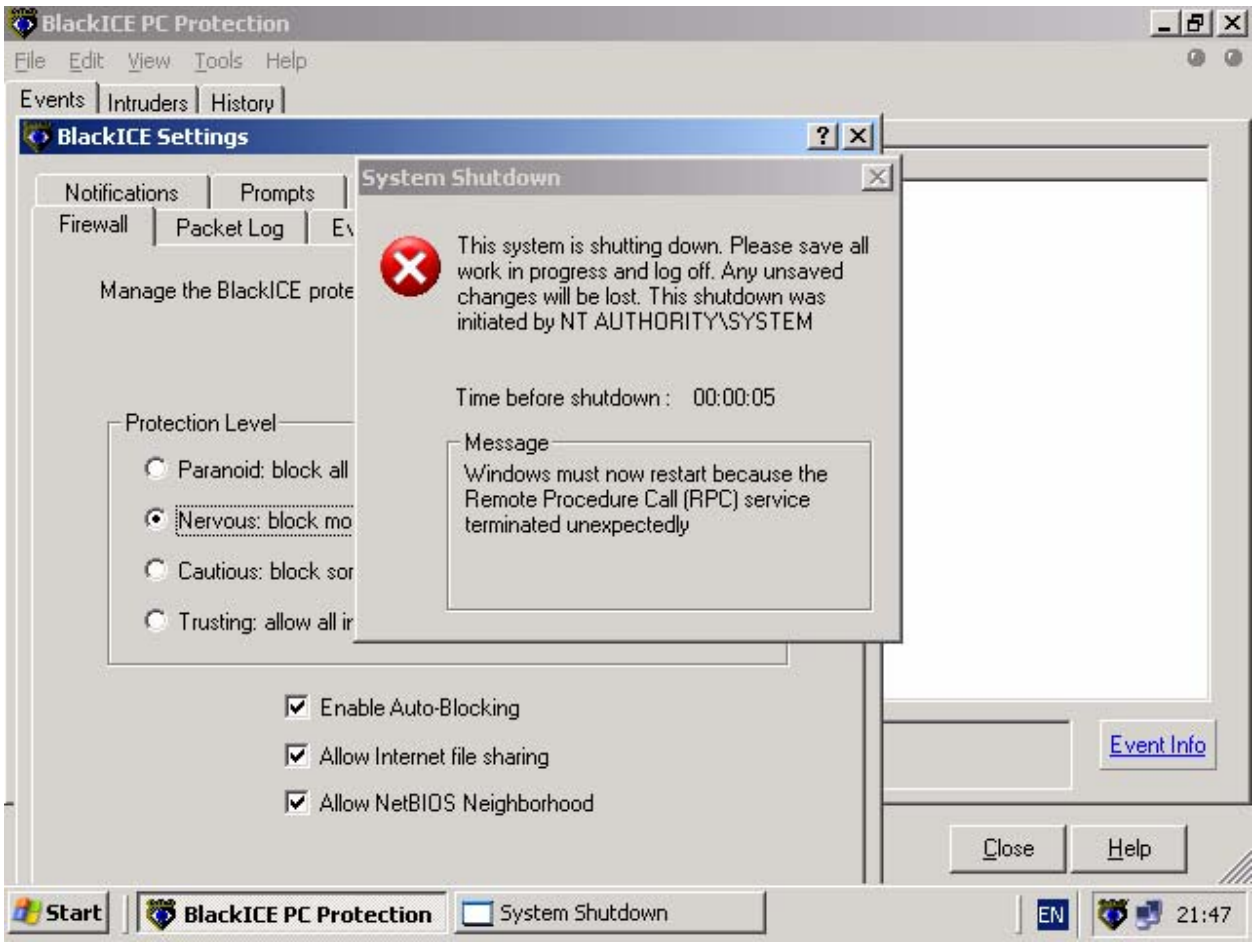

Рисунок 47. COA Black ICE пропускает DoS-атаку, вызванную эксплойтом, использующим уязвимость DCOM RPC Buffer Overflow, что приводит к перезагрузке ОС.

После обновления баз данных сигнатур, системы защиты успешно отражают эксплойты (рис. 48).

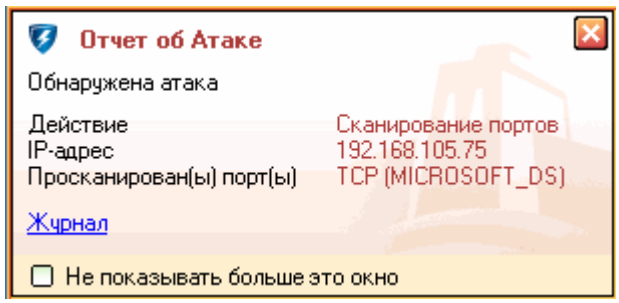

Рисунок 48. МЭ Agnitum Outpost PRO сообщает об обнаружении и отражении атаки, вызванной эксплойтом, использующему уязвимость MS04-007-dos в библиотеке Microsoft Windows ASN.1

Если выполнить обновление сигнатур МЭ или СОА невозможно, то временно нейтрализовать атаки можно лишь полной блокировкой трафика на уязвимые службы, например RPC, что очевидно не всегда осуществимо без потерь функциональности ОС.

Противодействие троянским программам, сетевым червям и вирусам

Эффективным методом противодействия трем данным видам угроз является использование антивирусных средств, работающих в режиме реального времени (мониторов). Для выявления троянских программ существует специализированное ПО (например Tauscan от Agnitum), однако, как показывает практика, современные антивирусы успешно обнаруживают и всевозможных троянских программ, и эксплойты (рис. 49).

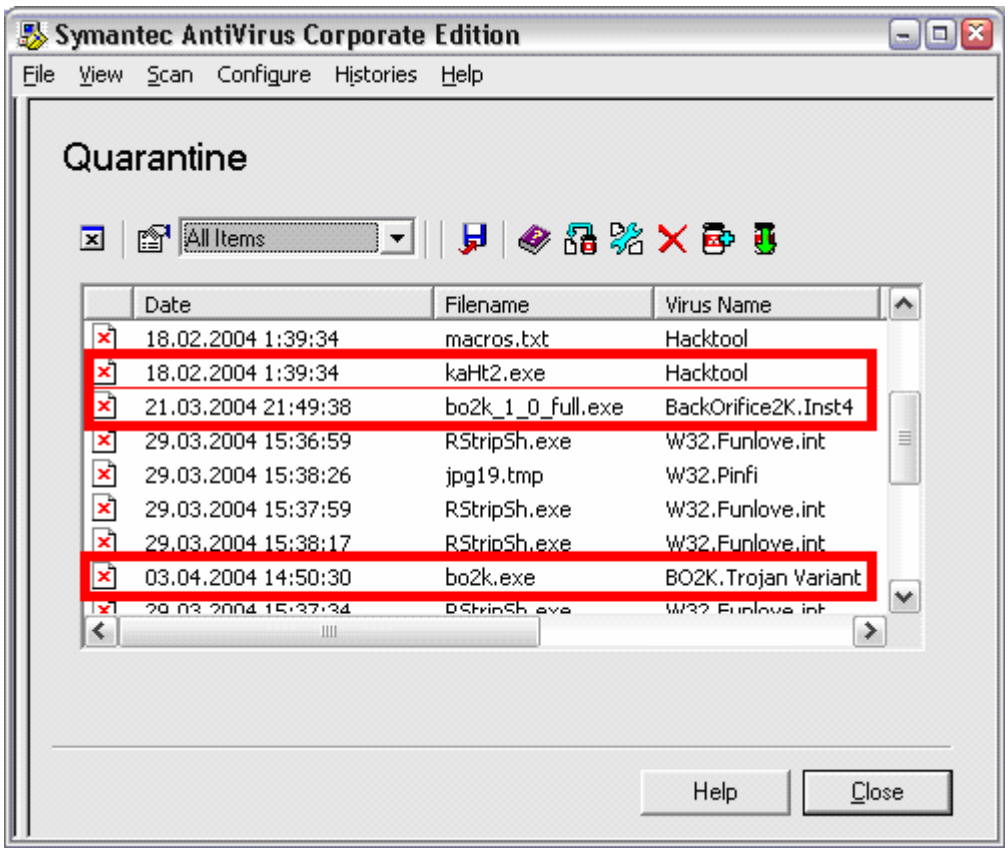

Рисунок 49. Антивирус Symantec Antivirus Server 8.1 обнаружил и поместил в карантин эксплойт kaHt2 и троянскую программу Back Orifice 2000.

Дополнительным препятствием для троянских программ является персональный МЭ. При попытке программы – троянского коня осуществить выход в сеть, МЭ в соответствии с настроенными правилами его работы, либо блокирует данное обращение, либо выведет уведомление для текущего пользователя (рис. 50).

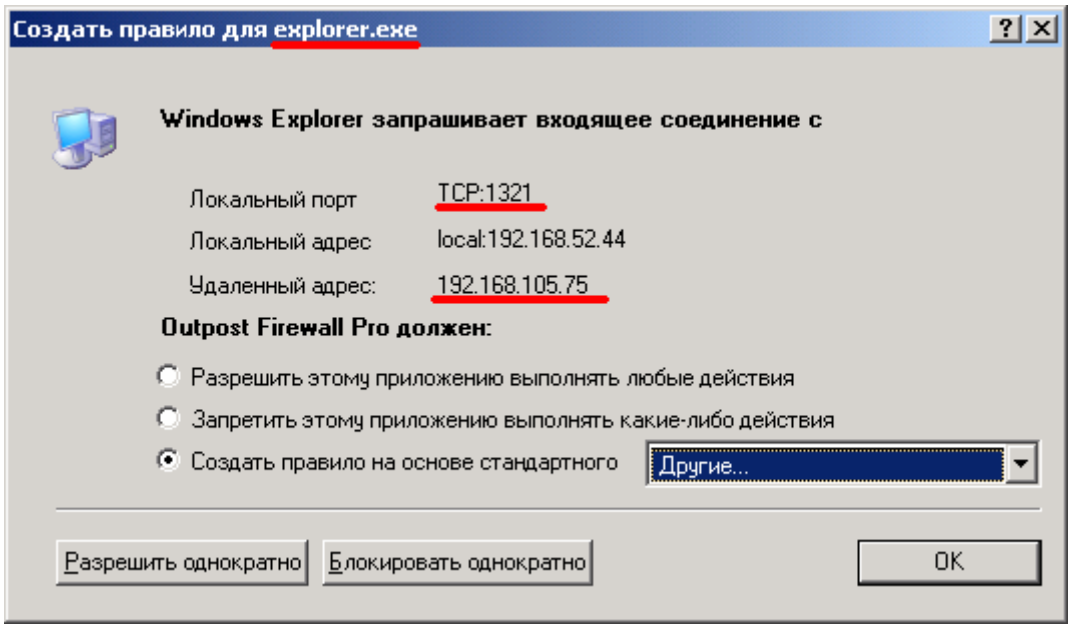

Рисунок 50. МЭ Agnitum Outpost предупреждает о том, что с приложением explorer.exe (под которое замаскировалась троянская программа Back Orifice) пытается установить соединение с удаленным хостом 192.168.105.75

В заключение описания методов защиты от активных воздействий, приведем ряд рекомендаций по тому, как определить, что кто-то удаленно подключился к Вашей системе, используя троянскую программу или эксплойты:

1. Троянские программы и эксплойты для удаленного управления системой открывают определенный порт и устанавливают с ним

соединение. Чаще всего это порт имеет номер больше 1024, т.е. лежит в диапазоне портов, не закрепленных жестко за определенной службой. Посмотреть открытые порты и заметить аномалию в Windows можно командой netstat –an (рис. 51).

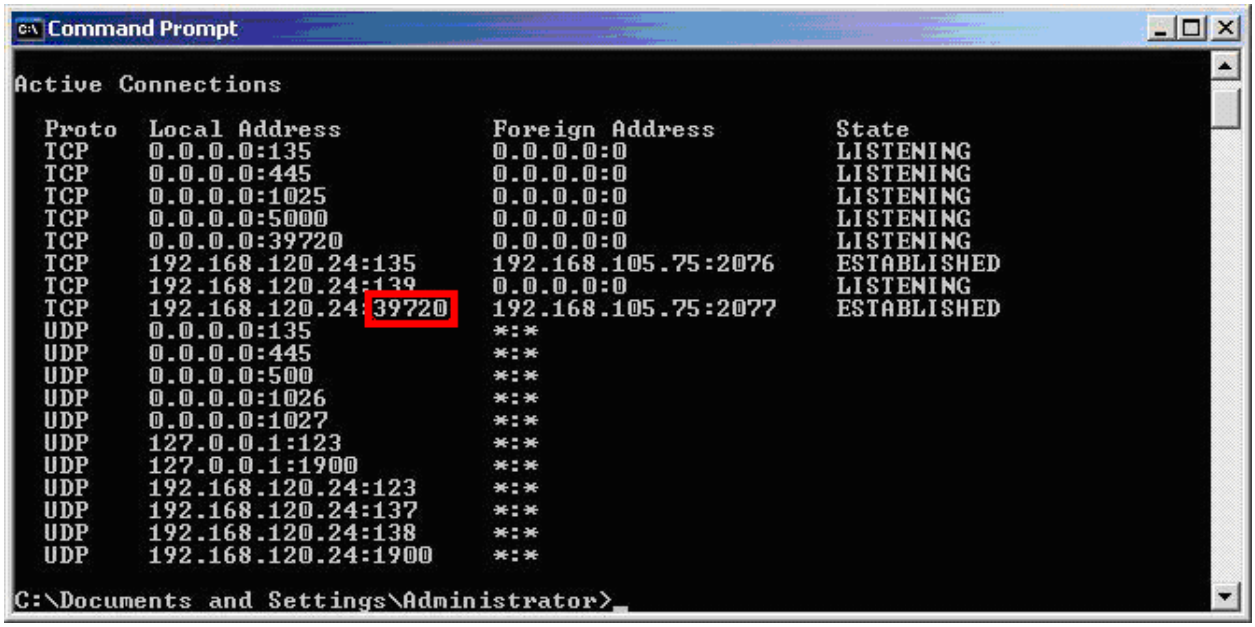

Рисунок 51. Злоумышленник, используя эксплойт kaHT2 открыл на удаленной системе порт 39720 для удаленного управления ею и установил с этим портом соединение (состояние established).

2. Как было отмечено выше, если эксплойт направлен на получение несанкционированного доступа к удаленной системе, то он чаще всего организовывает удаленный доступ посредством командной оболочки (также известной как shell или консоль), открытой на удаленной системе с правами учетной записи SYSTEM. Поскольку в нормальном режиме функционирования консоль с правами SYSTEM не может быть запущена, то подобную аномалию в случае применения эксплойта заметить легко (рис. 52). Следует отметить, что принудительное завершение процесса CMD.EXE из окна Windows Task Manager может в ряде случаев привести к вынужденной перезагрузке Windows (это зависит от того, в какой службе Windows была использована уязвимость).

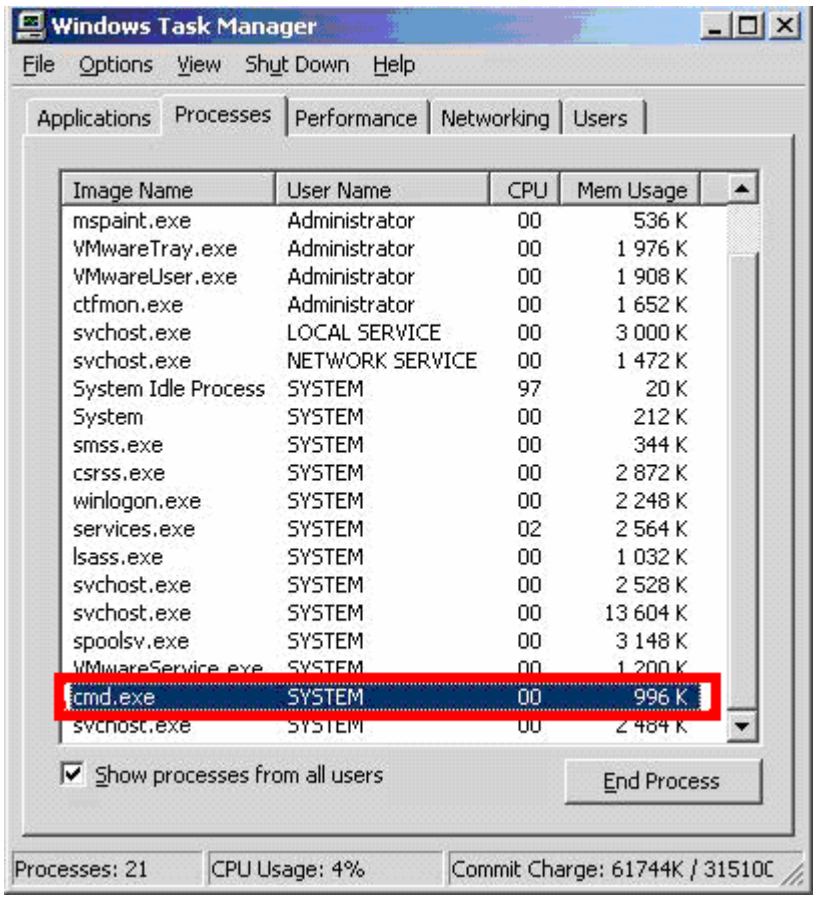

Рисунок 52. На системе, к которой был применен эксплойт, в списке запущенных процессов присутствует консоль, запущенная от имени учетной записи SYSTEM, что в MS Windows является аномальным.

Как следствие того, что командная оболочка, вызванная действием эксплойта, запускается с правами учетной записи SYSTEM, соответствующей самой ОС, обнаружить удаленно подключившегося посредством эксплойта пользователя из окна «Активные пользователи» невозможно (рис. 53).

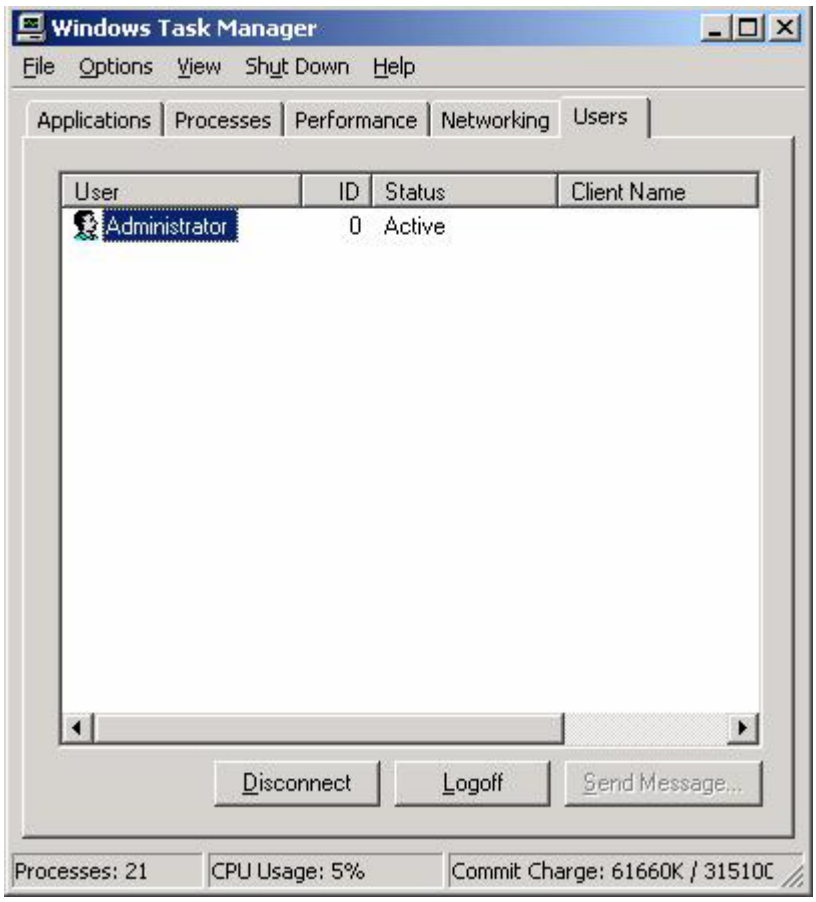

Рисунок 53. Несмотря на то, что к системе подключился удаленный пользователь, во вкладке «Users» отображается только администратор скомпрометированной системы.

Обнаружение утилит для сокрытия факта компрометации системы

Как показано выше, подобные утилиты не позволяют стандартными средствами ОС определить их наличие. Для их обнаружения разработаны специальные программы, например, Rootkit Hunter (Linux/Unix) или Patchfinder (Windows) (рис. 54).

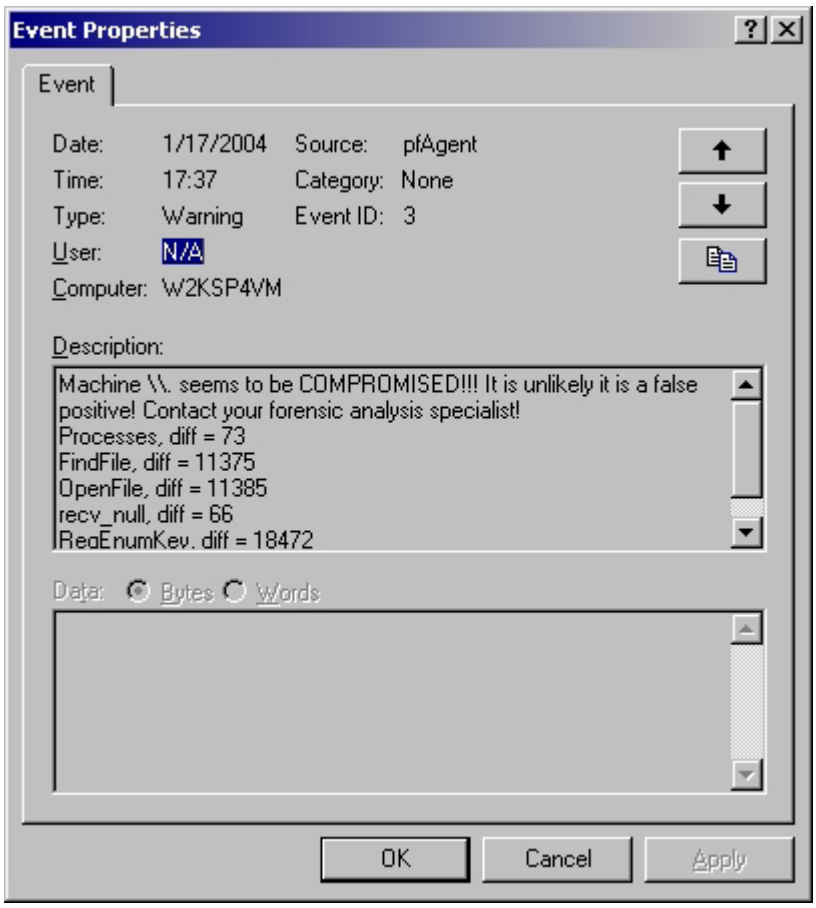

Рисунок 54. Программа Patchfinder обнаружила популярный rootkit HackerDefender для Windows, запущенный на локальной системе.

Также дополнительным препятствием являются антивирусные программы. Антивирусные мониторы часто определяют известные (т.е. занесенные в базы) программы для генерации таких патчей, как троянские. Например, антивирус Касперского определяет рассмотренный AFX Windows Rootkit 2003, как троянскую программу *Troyan.Win32.Madtol.a* и предлагает удалить этот объект (рис.55). Однако если патч уже был установлен, то антивирусная программа обнаруживает его в памяти, но попытка удаления/лечения приводит к бесконечной перезагрузке системы, так как патч очень глубоко интегрируется в ОС.

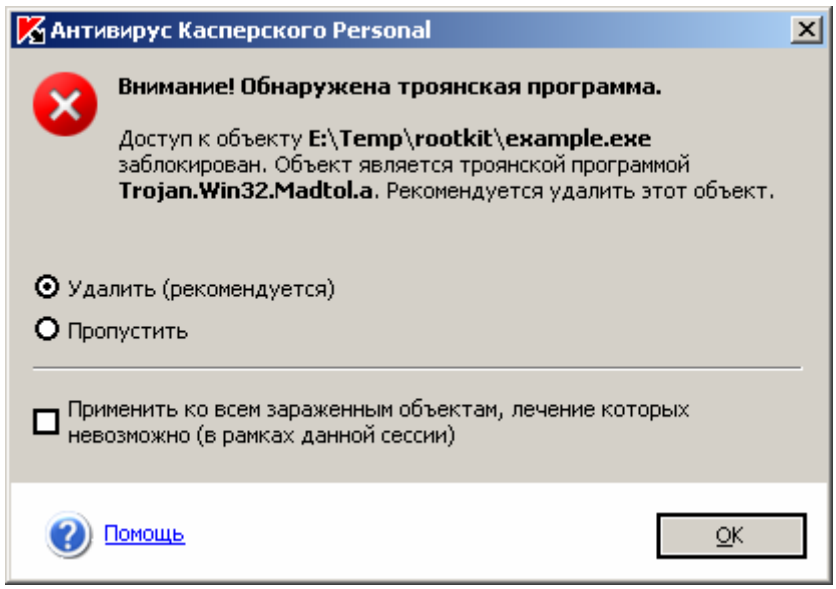

Рисунок 55. Антивирус Касперского обнаружил AFX Windows Rootkit 2003.

Противодействие несанкционированной установке модемов

Для предотвращения установки пользователями любого технического оборудования необходимо предусмотреть меры трех уровней – организационного, физического и программно-аппаратного. На организационном уровне необходимо в политике безопасности запретить сотрудникам подобные действия, установив меры ответственности. На физическом уровне меры защиты должны включать опечатывание всех свободных разъемов, портов компьютера. Аппаратные меры предусматривают отключение всех неиспользуемых модулей, разъемов. Возможна установка специализированных средств защиты, сигнализирующих о попытке вскрытия корпуса компьютера. Программные меры включают использования средств функционирующих на трех уровнях – уровне базовой системы ввода-вывода (BIOS), уровне ОС, уровне специализированных СЗИ. Поскольку стойкость средств защиты уровня BIOS и ОС остается низкой – существуют средства преодоления такой защиты, рекомендуется использования специализированных и особенно сертифицированных Гостехкомиссией России СЗИ, таких как Secret Net (НИП Информзащита), Spectr-M (СЦПС Спектр). Рассмотрим механизмы защиты от угроз изменения аппаратной конфигурации, реализованные в СЗИ Secret Net 2000. Функция системы «Контроль аппаратной конфигурации компьютера» предназначена для

своевременного обнаружения изменений конфигурации и выбора наиболее целесообразного способа реагирования на эти изменения.

Изменения аппаратной конфигурации компьютера могут быть вызваны: выходом из строя, добавлением или заменой отдельных устройств или всего компьютера. Для эффективного контроля конфигурации используется широкий набор контролируемых параметров, с каждым из которых связаны правила обнаружения изменений и действия, выполняемые в ответ на эти изменения. Сведения об аппаратной конфигурации компьютера хранятся в БД системы защиты. Первоначальные (эталонные) данные о конфигурации поступают от программы установки. Каждый раз при загрузке компьютера, а также при повторном входе пользователя система получает сведения об актуальной аппаратной конфигурации и сравнивает ее с эталонной. При обнаружении несоответствия анализируется серьезность возникающей ошибки и ее дальнейшее воздействие на безопасность информации. Контроль конфигурации программных и аппаратных средств производится ядром системы Secret Net. По результатам контроля ядро принимает решение о необходимости блокировки компьютера. Решение принимается после входа пользователя и зависит от настроек пользователя. Значение настроек пользователя определяет администратор безопасности. Если было выполнено запланированное изменение конфигурации компьютера, то пользователь, обладающий административными привилегиями, может при помощи подсистемы управления обновить эталонные сведения о конфигурации [35].

Системы централизованного мониторинга безопасности

Одним из методов автоматизации процессов анализа и контроля защищенности распределенных компьютерных систем является использование технологии интеллектуальных программных агентов. Система защиты строится на архитектуре консоль-менеджер-агент. На каждую из контролируемых систем устанавливается программный агент, который и выполняет соответствующие настройки ПО и проверяет их правильность, контролирует целостность файлов, своевременность установки пакетов программных коррекций, а также выполняет другие полезные задачи по контролю защищенности АС. (Управление агентами осуществляется по сети программой менеджером.) Менеджеры являются центральными компонентами подобных систем. Они посылают управляющие команды всем агентам контролируемого ими домена и сохраняют все данные, полученные от агентов в центральной базе данных. Администратор управляет менеджерами при помощи графической консоли, позволяющей выбирать, настраивать и создавать политики безопасности, анализировать изменения состояния системы, осуществлять ранжирование уязвимостей и т. п. Все взаимодействия между агентами, менеджерами и управляющей консолью осуществляются по защищенному клиент-серверному протоколу. Такой подход был использован при построении комплексной системы управления безопасностью организации Symantec Enterprise Security Manager, Tivoli IT Director.

Применение таких систем позволяет значительно повысить уровень защищенности в сети, однако высокая стоимость данных программных продуктов является сдерживающим фактором для их более широкого распространения.

Виртуальные ловушки

Интересным подходом к выявлению внутренних нарушителей является использование «виртуальных ловушек». «Виртуальные ловушки» – honeypots (горшочек меда), появились сравнительно недавно. Основная цель таких ловушек – стать приманкой для злоумышленника, принять атаку, сканирование и быть взломанной им.

Популярные виртуальные ловушки KFSensor и NFR Back Officer Friendly (BOF) способны эмулировать работу различных сервисов. Например, возможна эмуляция FTP-сервера, POP3-сервера, SMTP-сервера, TELNET-сервера, HTTP-сервера, SQL-сервера и многих других, в том числе серверной части троянской программы BackOrifice. При любой попытке доступа к данной службе выдается оповещение для администратора и протоколирование всей активности. Имеется возможность извещения администратора через электронную почту. KFSensor также предлагает разную степень эмуляции служб – от простой до максимально правдоподобной.

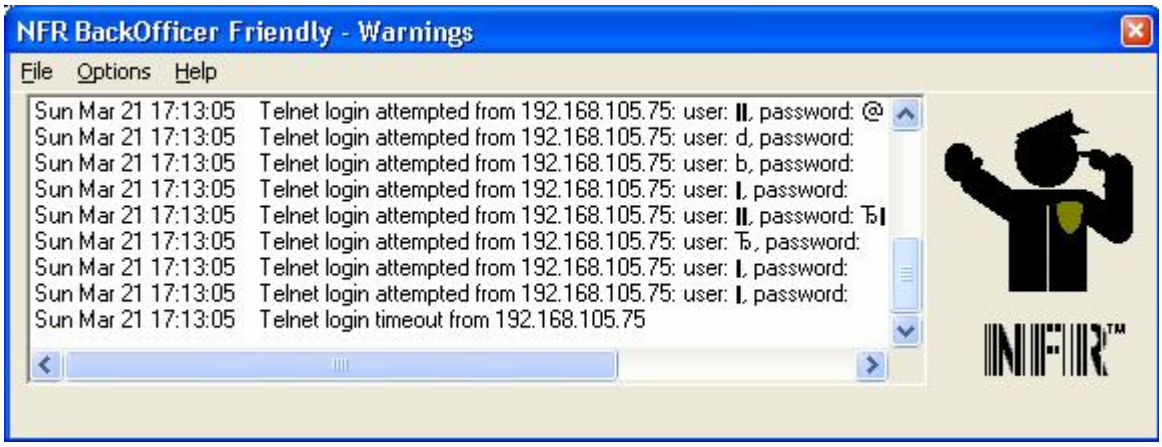

Рисунок 56. NFR BackOfficer Friendly, эмулирующий работу TELNET-сервера, оповещает о процессе подбора злоумышленником (IP-адрес 192.168.105.75) паролей к ложному серверу.

В качестве виртуальной ловушки использовать эмуляцию полноценного компьютера со своей ОС. Такая эмуляция осуществляется с использованием специального ПО – виртуальной машины. Наиболее известными продуктами из данной категории являются VMWare Workstation и Microsoft Virtual PC. Данные программы позволяют запускать на одном физическом компьютере множество ОС, полностью эмулируя их работу (рис 57).

Осуществляется поддержка разных версий Windows и Linux. Таким образом, механизм подготовки виртуальной ловушки заключается в установке ОС, выделении ей IP-адреса из диапазона адресов корпоративной сети и присвоение имени. Имя можно подобрать так, чтобы в первую очередь привлечь внимание потенциального нарушителя, например, mailserver или domain. Возможно эмулирование некоторых сервисных служб на виртуальной ловушке. Причем для эмуляции можно воспользоваться описанными выше KFSensor или BOF. Эмулируемую систему можно намеренно оставить уязвимой для применения эксплойтов, с целью проникновения злоумышленника. Анализ действия злоумышленника позволит определить что это – простое любопытство или направленная атака, а также точно установить его вину и объекты его интересов.

Таким образом, использование виртуальных ловушек для защиты корпоративной среды от внутренних нарушителей рекомендуется следующим образом:

1. Размещение ловушек, эмулирующих сервисы, на рабочих машинах администраторов и начальников вместе с рабочими сервисами.
2. Создание специальных серверов, полностью имитирующих уязвимые для атаки компьютеры.
3. Данные о польстившихся на легкую добычу использовать в защите всех машин своей сети. Часто менять имитацию уязвимых мест в сервисах.

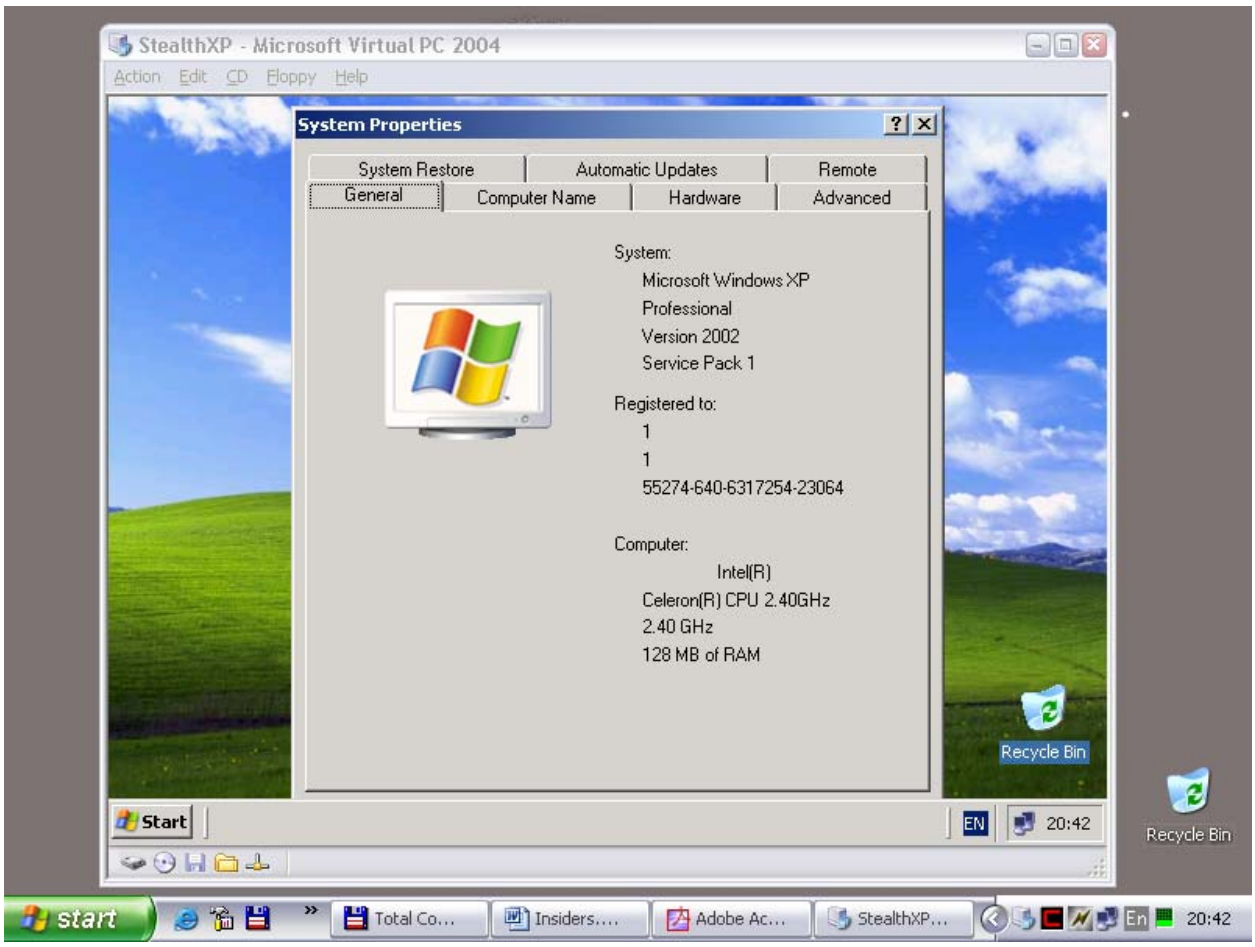

Рисунок 57. Эмуляция ОС Windows XP в виртуальной машине Microsoft Virtual PC, запущенной под управлением ОС Windows Server 2003.

Рекомендации по усилению защиты корпоративных сетей от внутренних нарушителей

На основании рассмотренных угроз и методов защиты сформулированы рекомендации, цель которых – снизить вероятность угроз, исходящих от внутренних нарушителей.

1. Заменить все имеющиеся в сети концентраторы на коммутаторы. Это позволит усложнить несанкционированное прослушивание трафика. Если позволяют финансовые возможности установить «интеллектуальные» управляемые коммутаторы 3-го уровня, обладающие расширенными возможностями в плане безопасности, например функцией port-security.
2. При использовании корпоративной почты рекомендуется задействовать механизмы шифрования, например, S/MIME или POP3S. Рекомендуется ограничить пользователям доступ к бесплатным электронным ящикам в Интернет.
3. Администраторам рекомендуется постоянно держать запущенными две программы: утилиту обнаружения атаки ARP-spoofing и сниффер, например, Cain, запущенный на маршрутизаторе или МЭ. Использование сниффера позволит увидеть сеть глазами потенциального нарушителя, выявить нарушителей политики безопасности.
4. Рекомендуется периодически анализировать защищенность корпоративной сети, используя сканеры уязвимостей.
5. Использовать шифрование сетевого трафика на прикладном, а лучше на сетевом уровне. Рекомендуется использование протокола IPSec.
6. Установить ПО, препятствующее запуску других программ, кроме назначенных администратором исходя из принципа: «Любому лицу предоставляются привилегии, необходимые для выполнения конкретных задач, но не больше». Все неиспользуемые порты компьютера должны быть аппаратно или программно дезактивированы. Это позволит значительно снизить вероятность всех угроз, осуществимых с рабочих станций пользователей. Поскольку, например, большинству снифферов для работы необходимо установить специальный драйвер. Существуют сертифицированные Гостехкомиссией средства защиты для локальных станций – Secret Net (НИП Информзащита), Spectr-M (СЦПС Спектр).

7. Для уменьшения риска угрозы расшифрования паролей рекомендуется:

- Активизация опции политики безопасности Windows «Password must meet complexity requirements»;
- Установка минимальной длины пароля в Windows 15 символов;
- Периодическая смена паролей;
- Обучение пользователей надежно хранить пароли.

8. Пользователь за своей рабочей станцией должен иметь пользовательские права.

9. Своевременное обновление всего ПО – для ОС, СОА, МЭ, антивирусного ПО значительно снижает риск использования эксплойтов, проникновения троянских программ, сетевых червей, вирусов.

10. Использование на рабочих местах по возможности и на серверах обязательно комплекта средств защиты – МЭ, СОА, антивирусное ПО. Лучше и удобнее, когда все составляющие от одного производителя, например, Symantec или Kaspersky. Если это дорого, можно обратится к ПО с открытыми исходными кодами – например, Snort. Есть и бесплатные антивирусы.

11. Важным элементом снижения возможного ущерба является процедура регулярного резервного копирования важной информации (backup).

12. Использование виртуальных ловушек для защиты корпоративной среды от внутренних нарушителей рекомендуется следующим образом:

- Размещение ловушек, эмулирующих сервисы, на рабочих машинах администраторов и начальников вместе с рабочими сервисами.
- Создание специальных серверов, полностью имитирующих уязвимые для атаки компьютеры.
- Данные о польстившихся на легкую добычу использовать в защите всех машин своей сети. Часто менять имитацию уязвимых мест в сервисах.

13. Стратегия безопасности корпоративной сети, контроль, архитектура, политика, стандарты, процедуры и руководящие указания должны определяться и внедряться с учетом возможности атак умного, рационального и иррационального недоброжелателя, имеющего намерение навредить данной компании.

14. Ответственность и привилегии должны быть распределены таким образом, чтобы не допустить частных лиц или группу вступивших в сговор частных лиц к неправомерному управлению процессами по методу составных ключей, что может привести к серьезному ущербу и потерям.

15. Все незанятые слоты (порты, разъемы) компьютеров должны быть опечатаны, отключены физически и программно. Это позволит снизить вероятность угрозы использования личных съемных носителей информации, таких как флэш-память и USB-винчестеры, а также предотвратит несанкционированное подключение модема.

Заключение

Согласно результатам исследования компании «Ibas», проведенного в январе 2004 года, 70% сотрудников воруют конфиденциальную информацию с рабочих мест**.** Больше всего с работы уносят такие вещи, как книги электронных адресов, базы данных клиентов, а также коммерческие предложения и презентации. И, более того, 72% опрошенных не страдают этическими проблемами, считая, что имеют законные права на нематериальное имущество компании. С другой стороны, согласно существующей статистике, в коллективах людей, занятых той или иной деятельностью, как правило, только около 85% являются вполне лояльными (честными), а остальные 15% делятся примерно так: 5% - могут совершить что-нибудь противоправное, если, по их представлениям, вероятность заслуженного наказания мала; 5% - готовы рискнуть на противоправные действия, даже если шансы быть уличенным и наказанным складываются 50% на 50%; 5% - готовы пойти на противозаконный поступок, даже если они почти уверены в том, что будут уличены и наказаны. Такая статистика в той или иной мере может быть применима к коллективам, участвующим в разработке и эксплуатации информационно-технических составляющих компьютерных систем. Таким образом, можно предположить, что не менее 5% персонала, участвующего в разработке и эксплуатации программных комплексов, способны осуществить действия криминального характера из корыстных побуждений либо под влиянием каких-нибудь иных обстоятельств. Следовательно, затронутая в работе проблема вполне актуальна. И только в последнее время компании, специализирующиеся на разработке средств защиты, осознали необходимость в разработке средств защиты от внутренних нарушителей. Одну из первых систем подобного рода выпустила отечественная компания «Праймтек» в конце 2003 года. Система предназначена для контроля политики безопасности организации.

Ярким примером актуальности проблемы защиты от внутренних нарушителей являются конфиденциальные базы данных по владельцам

недвижимости, движимости, телефонам, сводкам по криминалу и антикриминалу, базы данных ОВИР и многие другие, распространяемые нелегально на специализированных рынках в Москве и Санкт-Петербурге, а также через Интернет. Все эти базы похищаются недобросовестными сотрудниками, бороться с которыми власти пытаются организационными мерами. Так мэрия Москвы предлагает установить персональную ответственность соответствующих начальников отделов за нарушение конфиденциальности материалов государственных организаций.

Важно, что во многих организациях недооценивают опасность, исходящую от внутренних нарушителей. Как показало исследование, проведенное журналом eWeek, 57% респондентов и не полагали, что угрозы изнутри организации гораздо более реальны, чем извне. 22% исследуемых вообще не задумывались о такой угрозе. А в 43% организаций учетные записи уволенных сотрудников не удаляются.

Важным выводом является тот факт, что для совершения высокотехнологичного преступления злоумышленнику необязательно быть специалистом по информационным технологиям. Это означает, что практически любой сотрудник организации потенциально в состоянии нанести серьезный ущерб компании с использованием программных средств. Конкретные примеры иллюстрируют, что в сети Интернет можно найти огромное число обучающих материалов и готовых программных продуктов для реализации несанкционированного доступа к компьютерам в локальных вычислительных сетях. Многие статьи написаны доступным языком и снабжены подробными инструкциями по реализации атак. Однако проблема конечно не в наличие таких материалов, а в слабости современных технологий защиты сетей.

Список использованной литературы

1. Осовецкий Л.Г., Немолочнов О.Ф., Твердый Л.В., Беляков Д.А. Основы корпоративной теории информации. СПб: СПбГУ ИТМО, 2004
2. Гайкович В., Першин А. Безопасность банковских электронных систем, М.:1993
3. Наумов В. Отечественное законодательство в борьбе с компьютерными преступлениями // Computer World Россия, №8, 1997.
4. Гайкович В.Ю., Ершов Д.В. «Основы безопасности информационных технологий», – М.: МИФИ, 1995.
5. А. Астахов «Анализ защищенности корпоративных автоматизированных систем», Москва, информационный бюллетень Jet Info N7-2002
6. Лукацкий А.В. Как работает сканер безопасности. Hackzone, 1999
7. Александр Астахов «IDS как средство управления рисками» Internet URL http://www.globaltrust.ru/security/Pubs/Pub2_part5.htm
8. [А. В. Соколов, В. Ф. Шаньгин Защита информации в распределенных корпоративных сетях и системах, ДМК Пресс, 656 стр., 2002 г.
9. Internet URL http://www.robergraham.com/hacker-dictionary Hacker Dictionary
10. Deborah Russell, G. T. Gangemi, «Computer Security Basics», O'Reilly & Associates, Inc., Sebastopol, CA, 1991.
11. Крысин В.А. Безопасность предпринимательской деятельности. — М:Финансы и статистика, 1996 г.
12. Аджиев В. Мифы о безопасности программного обеспечения: уроки знаменитых катастроф. — Открытые системы, 1998 г., №6.
13. Internet URL http://www.globaltrust.ru/security/knowbase/Policies/Guide_Struct.htm «Структура руководства по обеспечению информационной безопасности»
14. Internet URL http://www.iitrust.ru/articles/zat_ibezop.htm "Как обосновать затраты на информационную безопасность?"
15. РД Гостехкомиссии «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»
16. Демин В.С. и др. Автоматизированные банковские системы. — М: Менатеп-Информ, 1997 г.
17. Whalen, Sean. "An Introduction to ARP Spoofing". Revision 1. April 2001

18. RFC 1734 POP3 Authentication command Internet URL http://www.faqs.org/rfcs/rfc1734.html
19. RFC 959 File Transfer Protocol Internet URL http://www.faqs.org/rfcs/rfc959.html
20. Internet URL http://www.securityfriday.com Cracking NTLMv2 Authentication
21. Internet URL www.hut.fi/~autikkan/kerberos/docs/phase1/pdf/LATEST_final_report.pdf Kimmo Kasslin Antti Tikkanen Attacks on Kerberos V in a Windows 2000 Environment 09.05.2003
22. Internet URL http://www.brd.ie Frank O'Dwyer Feasibility of attacking Windows 2000 Kerberos Passwords 05.03.2002
23. Internet URL http://lasecwww.epfl.ch/php_code/publications/search.php?ref=Oech03
24. Internet URL http://www.antsight.com/zsl/rainbowcrack/
25. Internet URL http://www.izone.kiev.ua Цифры на стороне Microsoft
26. Internet URL http://www.microsoft.com/technet/security/bulletin/ms03-026.mspx
27. Internet URL http://securityfriday.com Daiji Sanai Detection of Promiscuous Nodes Using ARP Packets 31.08.2001
28. Internet URL http://www.sans.org SANS Bulletin Why your switched network isn't secure
29. Internet URL http://www.sans.org Tom King Packet Sniffing In a Switched Environment, August 2002 SANS Institute
30. Internet URL http://www.securitylab.ru/33493.html arp_antidote - средство для активной борьбы с атаками типа arpoison
31. Internet URL http://www.securitylab.ru/34607.html IP Smart Spoofing - новый метод отравления ARP кэша, 27 ноября 2002 года
32. Д. Аникин Против кого работает служба безопасности? Безопасность.Достоверность.Информация. №3 2003 стр. 18-19
33. Internet URL http://www.securitylab.ru/29827.html Михаил Разумов «Десять мифов о паролях в Windows»
34. Internet URL http://www.securitylab.ru/40572.html «Сканирование. За и Против»
35. Internet URL http://www .infosec.ru НИП Информзащита «СЗИ Secret Net 2000. Принципы построения»

Список рекомендуемой литературы

Не надо читать много книг
Мао Цзе Дун

1. А. В. Соколов, В. Ф. Шаньгин Защита информации в распределенных корпоративных сетях и системах, ДМК Пресс, 656 стр., 2002 г.
2. Х. Остерлох TCP/IP. Семейство протоколов передачи данных в сетях компьютеров. «ДиаСофтЮП», 576 стр., 2002 г.
3. В. Зима, А. Молдовян, Н. Молдовян Безопасность глобальных сетевых технологий, БХВ-Санкт-Петербург, 368 стр., 2002 г.
4. А.В. Лукацкий Обнаружение атак, БХВ-Санкт-Петербург, 596 стр., 2003 г.
5. И. Д. Медведковский, Б. В. Семьянов, Д. Г. Леонов, А. В. Лукацкий Атака из Internet, 368 стр., 2002 г.
6. И. Конев, А. Беляев Информационная безопасность предприятия СПб-БХВ-Санкт-Петербург, 2003 – 752 с.
7. Д. Скляров Искусство защиты и взлома информации, БХВ-Петербург, 288 стр., 2004 г.
8. А. Ю. Щеглов Защита компьютерной информации от несанкционированного доступа, Наука и Техника, 384 стр., 2004 г.
9. В. В. Домарев Безопасность информационных технологий. Методология создания систем защиты, ТИД "ДС", 688 стр., 2002 г.
10. Ховард М., Лебланк Д. Защищенный код/Пер. с англ. – М.: Издательско-торговый дом «Русская редакция», 2003. – 704 стр.

Контрольные вопросы

1. Корпоративная теория информации. Понятие корпорации, ресурсов, системы, языковых связей. Понятие ценности корпоративной информации.
2. Проблемы безопасности корпоративных компьютерных систем.
3. Комплексный подход к обеспечению ИБ.
4. Принципы обеспечения ИБ.
5. Концепция обеспечения безопасности информационных ресурсов корпоративных сетей
6. Основные понятия корпоративной сети. Особенности корпоративных сетей
7. Особенности и классификационные признаки корпоративных сетей.
8. Обобщенная структура корпоративной сети.
9. Структура управления эффективностью корпоративной сети.
10. Структура управления безопасностью корпоративной сети.
11. Защищенность АС. Нормативная база анализа защищенности (Общие критерии, РД Гостехкомиссии, ISO17799).
12. Методика анализа защищенности. Исходные данные по обследуемой АС.
13. Анализ конфигурации средств защиты внешнего периметра ЛВС. Методы тестирования системы защиты. Сетевые сканеры. Механизмы работы сканеров безопасности.
14. Межсетевые экраны, классификация, политика работы, схемы подключения.
15. Системы обнаружения атак.
16. Виртуальные частные сети. Общий обзор.
17. Функции и компоненты сети VPN. Механизмы туннелирования и инкапсуляции.
18. Классификация VPN. Общий обзор
19. Классификация VPN по уровню модели OSI.
20. Классификация VPN по архитектуре технического решения. Классификация VPN по способу технического решения.
21. Технические и экономические преимущества внедрения технологий VPN в корпоративные сети
22. Характеристика внутренних нарушителей. Классификация методов воздействия внутренних нарушителей на корпоративные сети
23. Угрозы прослушивания сетевого трафика в корпоративных сетях на основе концентраторов и коммутаторов. Атаки ARP-spoofing, MAC-Flooding и MAC-Duplicating.
24. Последствия угрозы прослушивания сетевого трафика.

25. Использование внутренними злоумышленниками сканеров уязвимостей
26. Классификация сетевых атак. Сетевые атаки, основанные на использовании уязвимостей в ПО.
27. Троянские программы и утилиты для сокрытия фактов компрометации системы.
28. Вирусы и сетевые черви. Несанкционированная установка дополнительных программно-технических средств.
29. Методы противодействия угрозе прослушивания трафика. (обнаружение снифферов ARP- и Ping-методами не надо).
30. Методы, снижающие риск угрозы расшифрования паролей
31. Обнаружение сканирования. Противодействие эксплойтам.
32. Противодействие троянским программам, сетевым червям и вирусам. Обнаружение утилит Rootkits.
33. Противодействие несанкционированной установке модемов
34. Системы централизованного мониторинга безопасности и виртуальные ловушки.
35. Рекомендации по усилению защиты корпоративных сетей от внутренних нарушителей.

Кафедра
безопасных информационных технологий
(БИТ)
Санкт-Петербургского государственного
университета информационных технологий,
механики и оптики
(СПб ГУ ИТМО)

Кафедра Безопасные информационные технологии осуществляет подготовку специалистов по специальности 075300 – Организация и технология защиты информации. Квалификация: специалист по защите информации. Кафедра является базовой кафедрой Государственной технической комиссии при Президенте Российской Федерации и функционирует на базе органа по сертификации и аттестации по требованиям безопасности информации Научно-технического центра «Критические информационные технологии».

На кафедре БИТ осуществляется выполнение научно-исследовательских работ в области безопасности и защиты информации телекоммуникационных вычислительных систем, включающие:

1. Проведение анализа защищенности автоматизированных систем обработки данных и средств вычислительной техники.
2. Построение и проектирование комплексных систем защиты информации.
3. Сертификация средств защиты и автоматизированных систем с имеющимися средствами защиты на предмет соответствия определенному классу защищенности по руководящим документам (РД) Гостехкомиссии России.
4. Аттестация объектов информатизации.

Кафедра БИТ является разработчиком Концепции информационной безопасности региона, разработчиком Концепции защиты информации в банковских информационных технологиях.

Кафедра БИТ имеет большой опыт эксплуатации и внедрения средств защиты сетевого взаимодействия пользователей корпоративных сетей при подключении к общедоступным каналам связи (в том числе Интернет). Для обеспечения безопасного взаимодействия клиентов и защиты ресурсов собственной корпоративной сети предлагаются высокоэффективные решения на базе сертифицированных Гостехкомиссией России средств защиты информации. К таковым относятся межсетевые экраны, функционирующие на базе различных UNIX-платформ, защищенные программные маршрутизаторы, позволяющие организовывать виртуальные частные сети и ряд других

средств, обеспечивающих безопасное сетевое взаимодействие. Указанные средства имеют гибкие механизмы настройки под определенную конфигурацию сети и требования пользователей. Специалисты кафедры БИТ проводили сертификационные испытания множества сетевых средств защиты, что позволяет им наиболее полно использовать достоинства каждой из систем в целях достижения максимальной степени защищенности и удобства для Заказчика.

Специалисты кафедры БИТ ведут научные работы по созданию новой технологической схемы защиты информации от вирусных воздействий, по созданию иммунной системы защиты, методические исследования в области проведения сертификационных испытаний средств защиты и автоматизированных систем обработки информации с имеющимися системами защиты.

Специалисты кафедры БИТ являются авторами некоторых основополагающих Руководящих Документов Гостехкомиссии России.

Результаты научных работ и исследований, полученные специалистами кафедры БИТ, неоднократно обсуждались в научных статьях, опубликованы в ряде российских научно-технических и специализированных журналах, а также докладывались на многих конференциях, посвященных вопросам обеспечения информационной безопасности как в России, так и за рубежом.

Кафедрой заключены договора о сотрудничестве и ведутся работы с ведущими западными фирмами в области информационных технологий (Oracle, CyberGuard, Ericsson, Internet Security Systems, Microsoft).

Возглавляет кафедру БИТ Осовецкий Леонид Георгиевич, доктор технических наук, профессор, академик Международной Академии Информатизации, лауреат Государственной Премии СССР.

БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ СЕТЕЙ

Учебное пособие.

Тимур Александрович Биячуев

под редакцией
Леонида Георгиевича Осовецкого

В авторской редакции
Компьютерная верстка и дизайн Т.А. Биячуев
Дизайн обложки П.А. Гречников
Зав. РИО Н.Ф. Гусарова
Лицензия ИД №00408 от 05.11.99 Подписано к печати 25.09.04
Отпечатано на ризографе. Заказ №726. Тираж 100 экз.

Редакционно-издательский отдел
Санкт-Петербургского государственного
университета информационных технологий,
механики и оптики
197101, Санкт-Петербург, ул. Саблинская, 14