Содержание

Введение
1. Основные положения теории защиты информации
1.1 Классификация угроз безопасности информации
1.2 Наиболее распространенные угрозы
1.3 Программные атаки
1.4 Вредоносное программное обеспечение
1.5 Классификация мер обеспечения безопасности КС
2. Основные методы и средства защиты информации в сетях
2.1 Физическая защита информации
2.2 Аппаратные средства защиты информации в КС
2.3 Программные средства защиты информации в КС
3. Методы и средства защиты информации в телекоммуникационных сетях предприятия «Вестел»
3.1 Характеристика предприятия и корпоративной сети
3.2 Организационно-правовое обеспечение защиты информации
3.3 Защита информации в корпоративной сети «Вестел» на уровне операционной системы
3.4 Защита информации от несанкционированного доступа
3.5 Антивирусная защита
Заключение
Глоссарий
Список использованных источников
Список сокращений
Приложение А
Приложение Б
Приложение В
Приложение Г

Введение

Проблема защиты информации является далеко не новой. Решать её люди пытались с древних времен.

На заре цивилизации ценные сведения сохранялись в материальной форме: вырезались на каменных табличках, позже записывались на бумагу. Для их защиты использовались такие же материальные объекты: стены, рвы.

Информация часто передавалась с посыльным и в сопровождении охраны. И эти меры себя оправдывали, поскольку единственным способом получения чужой информации было ее похищение. К сожалению, физическая защита имела крупный недостаток. При захвате сообщения враги узнавали все, что было написано в нем. Еще Юлий Цезарь принял решение защищать ценные сведения в процессе передачи. Он изобрел шифр Цезаря. Этот шифр позволял посылать сообщения, которые никто не мог прочитать в случае перехвата.

Данная концепция получила свое развитие во время Второй мировой войны. Германия использовала машину под названием Enigma для шифрования сообщений, посылаемых воинским частям.

Конечно, способы защиты информации постоянно меняются, как меняется наше общество и технологии. Появление и широкое распространение компьютеров привело к тому, что большинство людей и организаций стали хранить информацию в электронном виде. Возникла потребность в защите такой информации.

В начале 70-х гг. XX века Дэвид Белл и Леонард Ла Падула разработали модель безопасности для операций, производимых на компьютере. Эта модель базировалась на правительственной концепции уровней классификации информации (несекретная, конфиденциальная, секретная, совершенно секретная) и уровней допуска. Если человек (субъект) имел уровень допуска выше, чем уровень файла (объекта) по классификации, то он получал доступ к файлу, в противном случае доступ отклонялся. Эта концепция нашла свою реализацию в стандарте 5200.28 "Trusted Computing System Evaluation Criteria" (TCSEC) ("Критерий оценки безопасности компьютерных систем"), разработанном в 1983 г. Министерством обороны США. Из-за цвета обложки он получил название "Оранжевая книга".

"Оранжевая книга" определяла для каждого раздела функциональные требования и требования гарантированности. Система должна была удовлетворять этим требованиям, чтобы соответствовать определенному уровню сертификации.

Выполнение требований гарантированности для большинства сертификатов безопасности отнимало много времени и стоило больших денег. В результате очень мало систем было сертифицировано выше, чем уровень C2 (на самом деле только одна система за все время была сертифицирована по уровню A1 - Honeywell SCOMP).[1]

При составлении других критериев были сделаны попытки разделить функциональные требования и требования гарантированности. Эти разработки вошли в "Зеленую книгу" Германии в 1989 г., в "Критерии Канады" в 1990 г., "Критерии оценки безопасности информационных технологий" (ITSEC) в 1991 г. и в "Федеральные критерии" (известные как Common Criteria - "Общие критерии") в 1992 г. Каждый стандарт предлагал свой способ сертификации безопасности компьютерных систем.

---

[1] Коул Э. Руководство по защите от хакеров. - М.: Издательский дом "Вильямс", 2002 - С. 25

Одна из проблем, связанных с критериями оценки безопасности систем, заключалась в недостаточном понимании механизмов работы в сети. При объединении компьютеров к старым проблемам безопасности добавляются новые. В "Оранжевой книге" не рассматривались проблемы, возникающие при объединении компьютеров в общую сеть, поэтому в 1987 г. появилась TNI (Trusted Network Interpretation), или "Красная книга". В "Красной книге" сохранены все требования к безопасности из "Оранжевой книги", сделана попытка адресации сетевого пространства и создания концепции безопасности сети. К сожалению, и "Красная книга" связывала функциональность с гарантированностью. Лишь некоторые системы прошли оценку по TNI, и ни одна из них не имела коммерческого успеха.

В наши дни проблемы стали еще серьезнее. Организации стали использовать беспроводные сети, появления которых "Красная книга" не могла предвидеть. Для беспроводных сетей сертификат "Красной книги" считается устаревшим.

Технологии компьютерных систем и сетей развиваются слишком быстро. Соответственно, также быстро появляются новые способы защиты информации. Поэтому тема моей квалификационной работы «Методы и средства защиты информации в сетях» является весьма актуальной.

Объектом исследования является информация, передаваемая по телекоммуникационным сетям.

Предметом исследования является информационная безопасность сетей.

Основной целью квалификационной работы является изучение и анализ методов и средств защиты информации в сетях.

Для достижения указанной цели необходимо решить ряд задач:

Рассмотреть угрозы безопасности и их классификацию;

Охарактеризовать методы и средства защиты информации в сети, их классификацию и особенности применения;

Раскрыть возможности физических, аппаратных и программных средств защиты информации в КС, выявить их достоинства и недостатки;

Рассмотреть методы, способы и средства защиты информации в корпоративной сети (на примере предприятия Вестел).

1. Основные положения теории защиты информации

1.1 Классификация угроз безопасности информации

Под угрозой безопасности информации в компьютерной сети (КС) понимают событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации[2].

Уязвимость информации — это возможность возникновения такого состояния, при котором создаются условия для реализации угроз безопасности информации.

Атакой на КС называют действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости. Иначе говоря, атака на КС является реализацией угрозы безопасности информации в ней.

Проблемы, возникающие с безопасностью передачи информации при работе в компьютерных сетях, можно разделить на три основных типа [4]:

· перехват информации – целостность информации сохраняется, но её конфиденциальность нарушена;

· модификация информации – исходное сообщение изменяется либо полностью подменяется другим и отсылается адресату;

· подмена авторства информации. Данная проблема может иметь серьёзные последствия. Например, кто-то может послать письмо от чужого имени (этот вид обмана принято называть спуфингом) или Web – сервер может притворяться электронным магазином, принимать заказы, номера кредитных карт, но не высылать никаких товаров.

---

[2] Норткат С., Новак Дж. Обнаружение нарушений безопасности в сетях. 3-е изд. - М.: Издательский дом "Вильямс", 2003, с. 23.

Специфика компьютерных сетей, с точки зрения их уязвимости, связана в основном с наличием интенсивного информационного взаимодействия между территориально разнесенными и разнородными (разнотипными) элементами.

Уязвимыми являются буквально все основные структурно-функциональные элементы КС: рабочие станции, серверы (Host-машины), межсетевые мосты (шлюзы, центры коммутации), каналы связи и т.д.

Известно большое количество разноплановых угроз безопасности информации различного происхождения. В литературе встречается множество разнообразных классификаций, где в качестве критериев деления используются виды порождаемых опасностей, степень злого умысла, источники появления угроз и т.д. Одна из самых простых классификаций приведена на рис. 1.

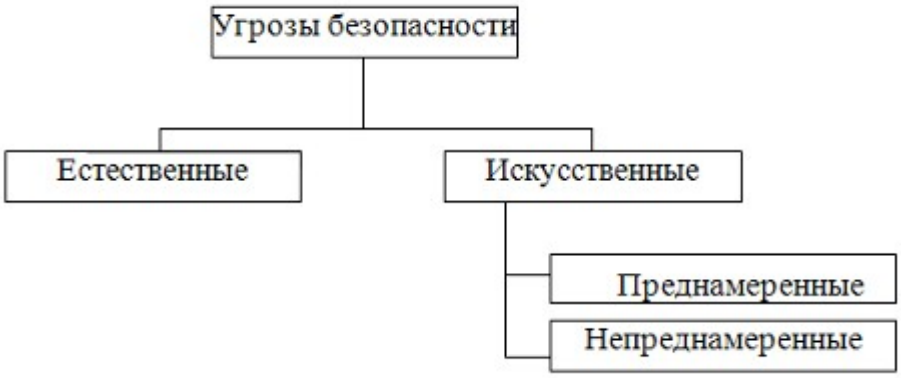


Рис. 1. Общая классификация угроз безопасности.

Естественные угрозы - это угрозы, вызванные воздействиями на КС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы - это угрозы КС, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании КС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;

преднамеренные (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Источники угроз по отношению к КС могут быть внешними или внутренними (компоненты самой КС - ее аппаратура, программы, персонал).

Более сложная и детальная классификация угроз приведена в Приложении А.

Анализ негативных последствий реализации угроз предполагает обязательную идентификацию возможных источников угроз, уязвимостей, способствующих их проявлению и методов реализации. И тогда цепочка вырастает в схему, представленную на рис. 2.

Рис. 2. Модель реализации угроз информационной безопасности.[3]

[3] Вихорев С., Кобцев Р. Как определить источники угроз.//Открытые системы. – 2002. - №07-08.С.43.

Угрозы классифицируются по возможности нанесения ущерба субъекту отношений при нарушении целей безопасности [31]. Ущерб может быть причинен каким-либо субъектом (преступление, вина или небрежность), а также стать следствием, не зависящим от субъекта проявлений. Угроз не так уж и много. При обеспечении конфиденциальности информации это может быть хищение (копирование) информации и средств ее обработки, а также ее утрата (неумышленная потеря, утечка). При обеспечении целостности информации список угроз таков: модификация (искажение) информации; отрицание подлинности информации; навязывание ложной информации. При обеспечении доступности информации возможно ее блокирование, либо уничтожение самой информации и средств ее обработки.

Все источники угроз можно разделить на классы, обусловленные типом носителя, а классы на группы по местоположению (рис. 3а). Уязвимости также можно разделить на классы по принадлежности к источнику уязвимостей, а классы на группы и подгруппы по проявлениям (рис. 3б). Методы реализации можно разделить на группы по способам реализации (рис. 3в). При этом необходимо учитывать, что само понятие «метод», применимо только при рассмотрении реализации угроз антропогенными источниками. Для техногенных и стихийных источников это понятие трансформируется в понятие «предпосылка».

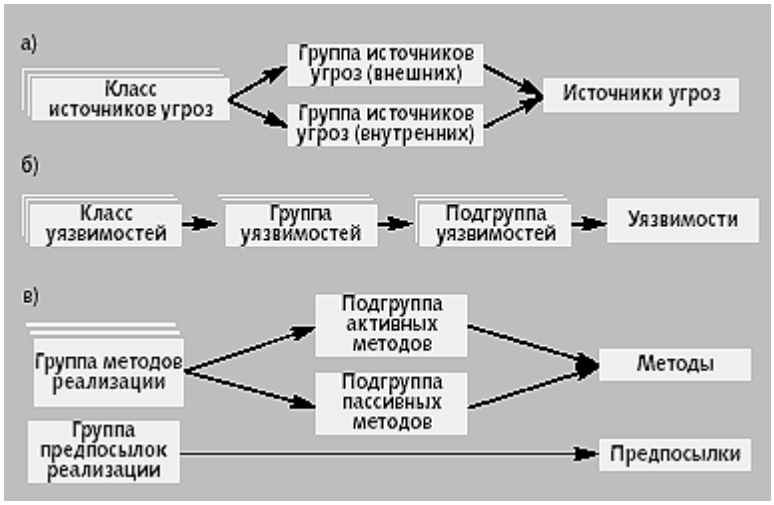


Рис. 3. Структура классификаций: а) «Источники угроз»; б) «Уязвимости»; в) «Методы реализации»

Классификация возможностей реализации угроз (атак), представляет собой совокупность возможных вариантов действий источника угроз определенными методами реализации с использованием уязвимостей, которые приводят к реализации целей атаки. Цель атаки может не совпадать с целью реализации угроз и может быть направлена на получение промежуточного результата, необходимого для достижения в дальнейшем реализации угрозы. В случае такого несовпадения атака рассматривается как этап подготовки к совершению действий, направленных на реализацию угрозы, т.е. как «подготовка к совершению» противоправного действия. Результатом атаки являются последствия, которые являются реализацией угрозы и/или способствуют такой реализации.

Исходными данными для проведения оценки и анализа угроз безопасности при работе в сети служат результаты анкетирования субъектов отношений, направленные на уяснение направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых в сети и условий расположения и эксплуатации сети.

1.2 Наиболее распространенные угрозы

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих компьютерную сеть [18].

Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь - следствие непреднамеренных ошибок.

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе.

Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками - максимальная автоматизация и строгий контроль.

Другие угрозы доступности можно классифицировать по компонентам КС, на которые нацелены угрозы:

отказ пользователей;

внутренний отказ сети;

отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);

невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);

невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками внутренних отказов являются:

отступление (случайное или умышленное) от установленных правил эксплуатации;

выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);

ошибки при (пере)конфигурировании системы;

отказы программного и аппаратного обеспечения;

разрушение данных;

разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы[4]:

нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;

разрушение или повреждение помещений;

невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые "обиженные" сотрудники - нынешние и бывшие. Как правило, они стремятся нанести вред организации - "обидчику", например:

испортить оборудование;

встроить логическую бомбу, которая со временем разрушит программы и/или данные;

удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

---

[4] Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. - СПб.: Питер, 2002, с. 247.

1.3 Программные атаки

В качестве средства вывода сети из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов (обычно - полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). По расположению источника угрозы такое потребление подразделяется на локальное и удаленное. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Простейший пример удаленного потребления ресурсов - атака, получившая наименование "SYN-наводнение" [5]. Она представляет собой попытку переполнить таблицу "полуоткрытых" TCP-соединений сервера (установление соединений начинается, но не заканчивается). Такая атака по меньшей мере затрудняет установление новых соединений со стороны легальных пользователей, то есть сервер выглядит как недоступный.

По отношению к атаке "Papa Smurf" уязвимы сети, воспринимающие ping-пакеты с широковещательными адресами. Ответы на такие пакеты "съедают" полосу пропускания.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме - как скоординированные распределенные атаки, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание. Временем начала "моды" на подобные атаки можно считать февраль 2000 года, когда жертвами оказались несколько крупнейших систем электронной коммерции (точнее - владельцы и пользователи систем). Если имеет место архитектурный просчет в виде разбалансированности между пропускной способностью сети и производительностью сервера, то защититься от распределенных атак на доступность крайне трудно.

Для выведения систем из штатного режима эксплуатации могут использоваться уязвимые места в виде программных и аппаратных ошибок. Например, известная ошибка в процессоре Pentium I давала возможность локальному пользователю путем выполнения определенной команды "подвесить" компьютер, так что помогает только аппаратный RESET [9].

Программа "Teardrop" удаленно "подвешивает" компьютеры, эксплуатируя ошибку в сборке фрагментированных IP-пакетов [23].

1.4 Вредоносное программное обеспечение

Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения.

Выделяют следующие аспекты вредоносного ПО:

вредоносная функция;

способ распространения;

внешнее представление.

Часть, осуществляющая разрушительную функцию, предназначается для:

внедрения другого вредоносного ПО;

получения контроля над атакуемой системой;

агрессивного потребления ресурсов;

изменения или разрушения программ и/или данных.

По механизму распространения различают:

вирусы - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;

"черви" - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по сети и их выполнение (для активизации вируса требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. "Черви", напротив, ориентированы в первую очередь на путешествия по сети.

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Например, "черви" "съедают" полосу пропускания сети и ресурсы почтовых систем.

Вредоносный код, который выглядит как функционально полезная программа, называется троянским. Например, обычная программа, будучи пораженной вирусом, становится троянской; порой троянские программы изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке[5] (обычно при посещении файлообменных сетей или игровых и развлекательных сайтов).

1.5 Классификация мер обеспечения безопасности КС

По способам осуществления все меры обеспечения безопасности компьютерных сетей подразделяются на: правовые (законодательные), морально-этические, организационные (административные), физические, технические (аппаратно-программные) [6,22].

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

---

[5] Бармен С. Разработка правил информационной безопасности. - М.: Издательский дом "Вильямс", 2002, с. 114.

К морально-этическим мерам противодействия относятся нормы поведения, которые традиционно сложились или складываются по мере распространения компьютерных сетей в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. Они включают [16]:

мероприятия, осуществляемые при проектировании, строительстве и оборудовании сетей и других объектов систем обработки данных;

мероприятия по разработке правил доступа пользователей к ресурсам сетей (разработка политики безопасности);

мероприятия, осуществляемые при подборе и подготовке персонала;

организацию охраны и надежного пропускного режима;

организацию учета, хранения, использования и уничтожения документов и носителей с информацией;

распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);

организацию явного и скрытого контроля за работой пользователей;

мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения и т.п.

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам сетей и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Технические (аппаратные) меры защиты основаны на использовании различных электронных устройств, входящих в состав КС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты.

Программные методы защиты предназначаются для непосредственной защиты информации по трем направлениям: а) аппаратуры; б) программного обеспечения; в) данных и управляющих команд.

Для защиты информации при ее передаче обычно используют различные методы шифрования данных перед их вводом в канал связи или на физический носитель с последующей расшифровкой. Как показывает практика, методы шифрования позволяют достаточно надежно скрыть смысл сообщения.

Все программы защиты, осуществляющие управление доступом к машинной информации, функционируют по принципу ответа на вопросы: кто может выполнять, какие операции и над какими данными.

Доступ может быть определен как:

общий (безусловно предоставляемый каждому пользователю);

отказ (безусловный отказ, например разрешение на удаление порции информации);

зависимый от события (управляемый событием);

зависимый от содержания данных;

зависимый от состояния (динамического состояния компьютерной системы);

частотно-зависимый (например, доступ разрешен пользователю только один или определенное число раз);

по имени или другим признаком пользователя;

зависимый от полномочий;

по разрешению (например, по паролю);

по процедуре.

Также к эффективным мерам противодействия попыткам несанкционированного доступа относятся средства регистрации. Для этих целей наиболее перспективными являются новые операционные системы специального назначения, широко применяемые в зарубежных странах и получившие название мониторинга (автоматического наблюдения за возможной компьютерной угрозой).

Мониторинг осуществляется самой операционной системой (ОС), причем в ее обязанности входит контроль за процессами ввода-вывода, обработки и уничтожения машинной информации. ОС фиксирует время несанкционированного доступа и программных средств, к которым был осуществлен доступ. Кроме этого, она производит немедленное оповещение службы компьютерной безопасности о посягательстве на безопасность компьютерной системы с одновременной выдачей на печать необходимых данных (листинга). В последнее время в США и ряде европейских стран для защиты компьютерных систем действуют также специальные подпрограммы, вызывающие самоуничтожение основной программы при попытке несанкционированного просмотра содержимого файла с секретной информацией по аналогии действия “логической бомбы”.

Задачи обеспечения безопасности[6]:

- защита информации в каналах связи и базах данных криптографическими методами;

---

[6] Зима В., Молдовян А., Молдовян Н. Безопасность глобальных сетевых технологий. – СПб.: BHV, 2000. С.56.

- подтверждение подлинности объектов данных и пользователей (аутентификация сторон, устанавливающих связь);

- обнаружение нарушений целостности объектов данных;

- обеспечение защиты технических средств и помещений, в которых ведется обработка конфиденциальной информации, от утечки по побочным каналам и от возможно внедренных в них электронных устройств съема информации;

- обеспечение защиты программных продуктов и средств вычислительной техники от внедрения в них программных вирусов и закладок;

- защита от несанкционированных действий по каналу связи от лиц, не допущенных к средствам шифрования, но преследующих цели компрометации секретной информации и дезорганизации работы абонентских пунктов;

- организационно-технические мероприятия, направленные на обеспечение сохранности конфиденциальных данных.

2. Основные методы и средства защиты информации в сетях

Разобрать подробно все методы и средства защиты информации в рамках ВКР просто невозможно. Охарактеризую только некоторые из них.

2.1 Физическая защита информации

К мерам физической защиты информации относятся:

защита от огня;

защита от воды и пожаротушащей жидкости

защита от коррозийных газов;

защита от электромагнитного излучения;

защита от вандализма;

защита от воровства и кражи;

защита от взрыва;

защита от падающих обломков;

защита от пыли;

защита от несанкционированного доступа в помещение.

Какие же действия нужно предпринять, чтобы обеспечить физическую безопасность?

В первую очередь надо подготовить помещение, где будут стоять серверы. Обязательное правило: сервер должен находиться в отдельной комнате, доступ в которую имеет строго ограниченный круг лиц. В этом помещении следует установить кондиционер и хорошую систему вентиляции. Там же можно поместить мини-АТС и другие жизненно важные технические системы.

Разумным шагом станет отключение неиспользуемых дисководов, параллельных и последовательных портов сервера. Его корпус желательно опечатать. Все это осложнит кражу или подмену информации даже в том случае, если злоумышленник каким-то образом проникнет в серверную комнату. Не стоит пренебрегать и такими тривиальными мерами защиты, как железные решетки и двери, кодовые замки и камеры видеонаблюдения, которые будут постоянно вести запись всего, что происходит в ключевых помещениях офиса.

Другая характерная ошибка связана с резервным копированием. О его необходимости знают все, так же как и о том, что на случай возгорания нужно иметь огнетушитель. А вот о том, что резервные копии нельзя хранить в одном помещении с сервером, почему-то забывают[7]. В результате, защитившись от информационных атак, фирмы оказываются беззащитными даже перед небольшим пожаром, в котором предусмотрительно сделанные копии гибнут вместе с сервером.

---

[7] Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие / под ред. Л.Г.Осовецкого - СПб.: СПбГУ ИТМО, 2004, с. 91.

Часто, даже защитив серверы, забывают, что в защите нуждаются и всевозможные провода - кабельная система сети. Причем, нередко приходится опасаться не злоумышленников, а самых обыкновенных уборщиц, которые заслуженно считаются самыми страшными врагами локальных сетей[8]. Лучший вариант защиты кабеля - это короба, но, в принципе, подойдет любой другой способ, позволяющий скрыть и надежно закрепить провода. Впрочем, не стоит упускать из вида и возможность подключения к ним извне для перехвата информации или создания помех, например, посредством разряда тока. Хотя, надо признать, что этот вариант мало распространен и замечен лишь при нарушениях работы крупных фирм.

Помимо Интернета, компьютеры включены еще в одну сеть - обычную электрическую. Именно с ней связана другая группа проблем, относящихся к физической безопасности серверов. Ни для кого не секрет, что качество современных силовых сетей далеко от идеального. Даже если нет никаких внешних признаков аномалий, очень часто напряжение в электросети выше или ниже нормы. При этом большинство людей даже не подозревают, что в их доме или офисе существуют какие-то проблемы с электропитанием.

Пониженное напряжение является наиболее распространенной аномалией и составляет около 85% от общего числа различных неполадок с электропитанием. Его обычная причина - дефицит электроэнергии, который особенно характерен для зимних месяцев. Повышенное напряжение почти всегда является следствием какой-либо аварии или повреждения проводки в помещении. Часто в результате отсоединения общего нулевого провода соседние фазы оказываются под напряжением 380 В. Бывает также, что высокое напряжение возникает в сети из-за неправильной коммутации проводов.

---

[8] Галатенко В.А. Стандарты информационной безопасности. - М.: Изд-во "Интернет-университет информационных технологий - ИНТУИТ.ру", 2004, с. 78.

Источниками импульсных и высокочастотных помех могут стать разряды молний, включение или отключение мощных потребителей электроэнергии, аварии на подстанциях, а также работа некоторых бытовых электроприборов. Чаще всего такие помехи возникают в крупных городах и в промышленных зонах. Импульсы напряжения при длительности от наносекунд (10~9 с) до микросекунд (10~6 с) могут по амплитуде достигать нескольких тысяч вольт. Наиболее уязвимыми к таким помехам оказываются микропроцессоры и другие электронные компоненты. Нередко непогашенная импульсная помеха может привести к перезагрузке сервера или к ошибке в обработке данных. Встроенный блок питания компьютера, конечно, частично сглаживает броски напряжения, защищая электронные компоненты компьютера от выхода из строя, но остаточные помехи все равно снижают срок службы аппаратуры, а также приводят к росту температуры в блоке питания сервера.

Для защиты компьютеров от высокочастотных импульсных помех служат сетевые фильтры (например, марки Pilot), оберегающие технику от большинства помех и перепадов напряжения. Кроме того, компьютеры с важной информацией следует обязательно оснащать источником бесперебойного питания (UPS). Современные модели UPS не только поддерживают работу компьютера, когда пропадает питание, но и отсоединяют его от электросети, если параметры электросети выходят из допустимого диапазона.

2.2 Аппаратные средства защиты информации в КС

К аппаратным средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к аппаратным, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств КС [3].

К основным аппаратным средствам защиты информации относятся:

• устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т.п.);

• устройства для шифрования информации;

• устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы).

Примеры вспомогательных аппаратных средств защиты информации:

• устройства уничтожения информации на магнитных носителях;

• устройства сигнализации о попытках несанкционированных действий пользователей КС и др.

Аппаратные средства привлекают все большее внимание специалистов не только потому, что их легче защитить от повреждений и других случайных или злоумышленных воздействий, но еще и потому, что аппаратная реализация функций выше по быстродействию, чем программная, а стоимость их неуклонно снижается.

На рынке аппаратных средств защиты появляются все новые устройства. Ниже приводится в качестве примера описание электронного замка.

Электронный замок «Соболь»

«Соболь», разработанный и поставляемый ЗАО НИП «Информзащита», обеспечивает выполнение следующих функций защиты:

идентификация и аутентификация пользователей;

контроль целостности файлов и физических секторов жесткого диска;

блокировка загрузки ОС с дискеты и CD-ROM;

блокировка входа в систему зарегистрированного пользователя при превышении им заданного количества неудачных попыток входа;

регистрация событий, имеющих отношение к безопасности системы.

Идентификация пользователей производится по индивидуальному ключу в виде «таблетки» Touch Memory, имеющей память до 64 Кбайт, а аутентификация — по паролю длиной до 16 символов.

Контроль целостности предназначен для того, чтобы убедиться, что программы и файлы пользователя и особенно системные файлы ОС не были модифицированы злоумышленником или введенной им программной закладкой. Для этого в первую очередь в работу вступает разборщик файловой системы ОС: расчет эталонных значений и их контроль при загрузке реализован в «Соболе» на аппаратном уровне. Построение же списка контроля целостности объектов выполняется с помощью утилиты ОС, что в принципе дает возможность программе-перехватчику модифицировать этот список, а ведь хорошо известно, что общий уровень безопасности системы определяется уровнем защищенности самого слабого звена.

2.3 Программные средства защиты информации в КС

Под программными средствами защиты информации понимают специальные программы, включаемые в состав программного обеспечения КС исключительно для выполнения защитных функций.

К основным программным средствам защиты информации относятся:

• программы идентификации и аутентификации пользователей КС;

• программы разграничения доступа пользователей к ресурсам КС;

• программы шифрования информации;

• программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования.

Надо понимать, что под идентификацией, применительно к обеспечению информационной безопасности КС, понимают однозначное распознавание уникального имени субъекта КС. Аутентификация означает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта)[9].

Также к программным средствам защиты информации относятся:

• программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т. п.);

• программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий;

• программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);

• программы тестового контроля защищенности КС и др.

К преимуществам программных средств защиты информации относятся:

• простота тиражирования;

• гибкость (возможность настройки на различные условия применения, учитывающие специфику угроз информационной безопасности конкретных КС);

• простота применения — одни программные средства, например шифрования, работают в «прозрачном» (незаметном для пользователя) режиме, а другие не требуют от пользователя ни каких новых (по сравнению с другими программами) навыков;

---

[9] Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие / под ред. Л.Г.Осовецкого - СПб.: СПбГУ ИТМО, 2004, с 64.

• практически неограниченные возможности их развития путем внесения изменений для учета новых угроз безопасности информации.

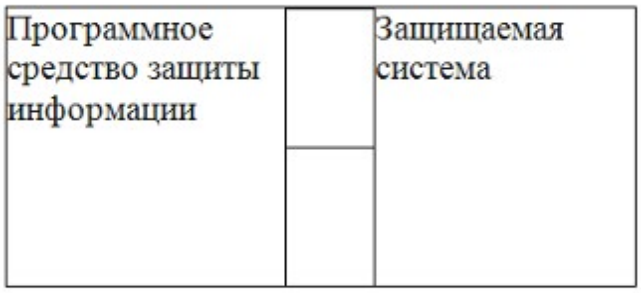


Рис. 4. Пример пристыкованного программного средства защиты.

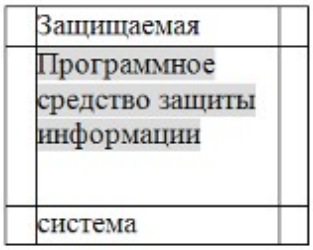


Рис. 5. Пример встроенного программного средства защиты.

К недостаткам программных средств защиты информации относятся:

• снижение эффективности КС за счет потребления ее ресурсов, требуемых для функционирование программ защиты;

• более низкая производительность (по сравнению с выполняющими аналогичные функции аппаратными средствами защиты, например шифрования);

• пристыкованность многих программных средств защиты (а не их встроенность в программное обеспечение КС, рис. 4 и 5), что создает для нарушителя принципиальную возможность их обхода;

• возможность злоумышленного изменения программных средств защиты в процессе эксплуатации КС.

Безопасность на уровне операционной системы

Операционная система является важнейшим программным компонентом любой вычислительной машины, поэтому от уровня реализации политики безопасности в каждой конкретной ОС во многом зависит и общая безопасность информационной системы [22].

Операционная система MS-DOS является ОС реального режима микропроцессора Intel, а потому здесь не может идти речи о разделении оперативной памяти между процессами. Все резидентные программы и основная программа используют общее пространство ОЗУ. Защита файлов отсутствует, о сетевой безопасности трудно сказать что-либо определенное, поскольку на том этапе развития ПО драйверы для сетевого взаимодействия разрабатывались не фирмой MicroSoft, а сторонними разработчиками.

Семейство операционных систем Windows 95, 98, Millenium – это клоны, изначально ориентированные на работу в домашних ЭВМ. Эти операционные системы используют уровни привилегий защищенного режима, но не делают никаких дополнительных проверок и не поддерживают системы дескрипторов безопасности. В результате этого любое приложение может получить доступ ко всему объему доступной оперативной памяти как с правами чтения, так и с правами записи. Меры сетевой безопасности присутствуют, однако, их реализация не на высоте. Более того, в версии Windows 95 была допущена основательная ошибка, позволяющая удаленно буквально за несколько пакетов приводить к "зависанию" ЭВМ, что также значительно подорвало репутацию ОС, в последующих версиях было сделано много шагов по улучшению сетевой безопасности этого клона[10].

[10] Зима В., Молдовян А., Молдовян Н. Безопасность глобальных сетевых технологий. Серия "Мастер". - СПб.: БХВ-Петербург, 2001, с. 124.

Поколение операционных систем Windows NT, 2000 уже значительно более надежная разработка компании MicroSoft. Они являются действительно многопользовательскими системами, надежно защищающими файлы различных пользователей на жестком диске (правда, шифрование данных все же не производится и файлы можно без проблем прочитать, загрузившись с диска другой операционной системы – например, MS-DOS). Данные ОС активно используют возможности защищенного режима процессоров Intel, и могут надежно защитить данные и код процесса от других программ, если только он сам не захочет предоставлять к ним дополнительного доступа извне процесса.

За долгое время разработки было учтено множество различных сетевых атак и ошибок в системе безопасности. Исправления к ним выходили в виде блоков обновлений (англ. service pack).

Другая ветвь клонов растет от операционной системы UNIX. Эта ОС изначально разрабатывалась как сетевая и многопользовательская, а потому сразу же содержала в себе средства информационной безопасности. Практически все широко распространенные клоны UNIX прошли долгий путь разработки и по мере модификации учли все открытые за это время способы атак. Достаточно себя зарекомендовали : LINUX (S.U.S.E.), OpenBSD, FreeBSD, Sun Solaris. Естественно все сказанное относится к последним версиям этих операционных систем. Основные ошибки в этих системах относятся уже не к ядру, которое работает безукоризненно, а к системным и прикладным утилитам. Наличие ошибок в них часто приводит к потере всего запаса прочности системы.

Основные компоненты:

Локальный администратор безопасности – несет ответственность за несанкционированный доступ, проверяет полномочия пользователя на вход в систему, поддерживает:

Аудит – проверка правильности выполнения действий пользователя

Диспетчер учетных записей – поддержка БД пользователей их действий и взаимодействия с системой.

Монитор безопасности – проверяет имеет ли пользователь достаточные права доступа на объект

Журнал аудита – содержит информацию о входах пользователей, фиксирует работы с файлами, папками.

Пакет проверки подлинности – анализирует системные файлы, на предмет того, что они не заменены. MSV10 – пакет по умолчанию.

Windows XP дополнена:

можно назначать пароли для архивных копий

средства защиты от замены файлов

система разграничения … путем ввода пароля и создания учета записей пользователя. Архивацию может проводить пользователь, у которого есть такие права.

NTFS: контроль доступа к файлам и папкам

В XP и 2000 – более полное и глубокое дифференцирование прав доступа пользователя.

EFS – обеспечивает шифрование и дешифрование информации (файлы и папки) для ограничения доступа к данным.

Криптографические методы защиты

Криптография - это наука об обеспечении безопасности данных. Она занимается поисками решений четырех важных проблем безопасности - конфиденциальности, аутентификации, целостности и контроля участников взаимодействия. Шифрование - это преобразование данных в нечитабельную форму, используя ключи шифрования-расшифровки. Шифрование позволяет обеспечить конфиденциальность, сохраняя информацию в тайне от того, кому она не предназначена.

Криптография занимается поиском и исследованием математических методов преобразования информации[11].

Современная криптография включает в себя четыре крупных раздела:

симметричные криптосистемы;

криптосистемы с открытым ключом;

системы электронной подписи;

управление ключами.

Основные направления использования криптографических методов - передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Шифрование дисков

Зашифрованный диск – это файл-контейнер, внутри которого могут находиться любые другие файлы или программы (они могут быть установлены и запущены прямо из этого зашифрованного файла). Этот диск доступен только после ввода пароля к файлу-контейнеру – тогда на компьютере появляется еще один диск, опознаваемый системой как логический и работа с которым не отличается от работы с любым другим диском. После отключения диска логический диск исчезает, он просто становится «невидимым».

На сегодняшний день наиболее распространенные программы для создания зашифрованных дисков – DriveCrypt, BestCrypt и PGPdisk. Каждая из них надежно защищена от удаленного взлома.

Общие черты программ:[12]

---

[11] Лапонина О.Р. Криптографические основы безопасности. - М.: Изд-во "Интернет-университет информационных технологий - ИНТУИТ.ру", 2004, с. 19.

[12] Ярочкин В.И. Информационная безопасность. - М. 2004. – С. 354-355.

- все изменения информации в файле-контейнере происходят сначала в оперативной памяти, т.е. жесткий диск всегда остается зашифрованным. Даже в случае зависания компьютера секретные данные так и остаются зашифрованными;

- программы могут блокировать скрытый логический диск по истечении определенного промежутка времени;

- все они недоверчиво относятся к временным файлам (своп-файлам). Есть возможность зашифровать всю конфиденциальную информацию, которая могла попасть в своп-файл. Очень эффективный метод скрытия информации, хранящейся в своп-файле – это вообще отключить его, при этом не забыв нарастить оперативную память компьютера;

- физика жесткого диска такова, что даже если поверх одних данных записать другие, то предыдущая запись полностью не сотрется. С помощью современных средств магнитной микроскопии (Magnetic Force Microscopy – MFM) их все равно можно восстановить. С помощью этих программ можно надежно удалять файлы с жесткого диска, не оставляя никаких следов их существования;

- все три программы сохраняют конфиденциальные данные в надежно зашифрованном виде на жестком диске и обеспечивают прозрачный доступ к этим данным из любой прикладной программы;

- они защищают зашифрованные файлы-контейнеры от случайного удаления;

- отлично справляются с троянскими приложениями и вирусами.

Способы идентификации пользователя

Прежде чем получить доступ к ВС, пользователь должен идентифицировать себя, а механизмы защиты сети затем подтверждают подлинность пользователя, т. е. проверяют, является ли пользователь действительно тем, за кого он себя выдает. В соответствии с логической моделью механизма защиты ВС размещены на рабочей ЭВМ, к которой подключен пользователь через свой терминал или каким-либо иным способом. Поэтому процедуры идентификации, подтверждения подлинности и наделения полномочиями выполняются в начале сеанса на местной рабочей ЭВМ.

В дальнейшем, когда устанавливаются различные сетевые протоколы и до получения доступа к сетевым ресурсам, процедуры идентификации, подтверждения подлинности и наделения полномочиями могут быть активизированы вновь на некоторых удаленных рабочих ЭВМ с целью размещения требуемых ресурсов или сетевых услуг.

Когда пользователь начинает работу в вычислительной системе, используя терминал, система запрашивает его имя и идентификационный номер. В соответствии с ответами пользователя вычислительная система производит его идентификацию. В сети более естественно для объектов, устанавливающих взаимную связь, идентифицировать друг друга.

Пароли - это лишь один из способов подтверждения подлинности. Существуют другие способы:

1. Предопределенная информация, находящаяся в распоряжении пользователя: пароль, личный идентификационный номер, соглашение об использовании специальных закодированных фраз.

2. Элементы аппаратного обеспечения, находящиеся в распоряжении пользователя: ключи, магнитные карточки, микросхемы и т.п..

3. Характерные личные особенности пользователя: отпечатки пальцев, рисунок сетчатки глаза, размеры фигуры, тембр голоса и другие более сложные медицинские и биохимические свойства.

4. Характерные приемы и черты поведения пользователя в режиме реального времени: особенности динамики, стиль работы на клавиатуре, скорость чтения, умение использовать манипуляторы и т.д.

5. Привычки: использование специфических компьютерных заготовок.

6. Навыки и знания пользователя, обусловленные образованием, культурой, обучением, предысторией, воспитанием, привычками и т.п.

Если кто-то желает войти в вычислительную систему через терминал или выполнить пакетное задание, вычислительная система должна установить подлинность пользователя. Сам пользователь, как правило, не проверяет подлинность вычислительной системы. Если процедура установления подлинности является односторонней, такую процедуру называют процедурой одностороннего подтверждения подлинности объекта[13].

Специализированные программные средства защиты информации

Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства сетевых ОС. Кроме программ шифрования, существует много других доступных внешних средств защиты информации. Из наиболее часто упоминаемых следует отметить следующие две системы, позволяющие ограничить информационные потоки.

Firewalls - брандмауэры (дословно firewall — огненная стена). Между локальной и глобальной сетями создаются специальные промежуточные сервера, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/ транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность совсем. Более защищенная разновидность метода - это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

---

[13] Денисов А., Белов А., Вихарев И. Интернет. Самоучитель. - СПб.: Питер, 2000, с 112.

Proxy-servers (proxy - доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью — попросту отсутствует маршрутизация как таковая, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом методе обращения из глобальной сети в локальную становятся невозможными в принципе. Очевидно также, что этот метод не дает достаточной защиты против атак на более высоких уровнях - например, на уровне приложения (вирусы, код Java и JavaScript).

Рассмотрим подробнее работу брандмауэра. Это метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами. Брандмауэр является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра). Брандмауэр конфигурируется в соответствии с принятой в организации политикой контроля доступа к внутренней сети. Все входящие и исходящие пакеты должны проходить через брандмауэр, который пропускает только авторизованные пакеты.

Брандмауэр с фильрацией пакетов [packet-filtering firewall] - является маршрутизатором или компьютером, на котором работает программное обеспечение, сконфигурированное таким образом, чтобы отбраковывать 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.).

Брандмауэр экспертного уровня [stateful inspecthion firewall] - проверяет содержимое принимаемых пакетов на трех уровнях модели OSI - сетевом, сеансовом и прикладном. Для выполнения этой задачи используются специальные алгоритмы фильтрации пакетов, с помощью которых каждый пакет сравнивается с известным шаблоном авторизованных пакетов.

Создание брандмауера относится к решению задачи экранирования. Формальная постановка задачи экранирования состоит в следующем. Пусть имеется два множества информационных систем. Экран - это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем (рис. 6). Контроль потоков состоит в их фильтрации, возможно, с выполнением некоторых преобразований.

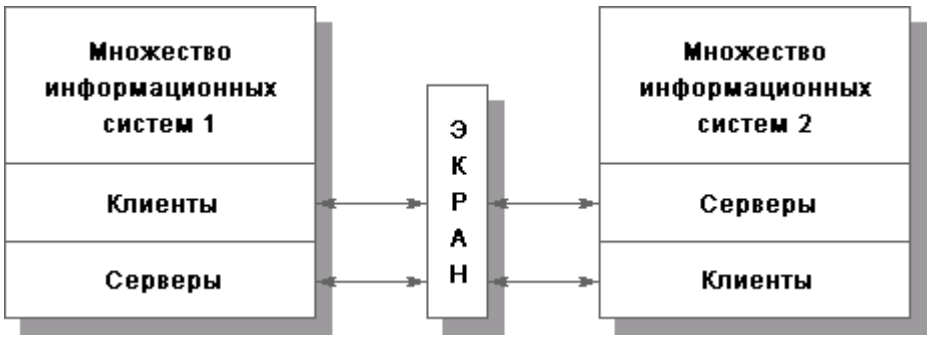

Множество информационных систем 1
Клиенты
Серверы
Э К Р А Н
Множество информационных систем 2
Серверы
Клиенты

Рис. 6. Экран как средство разграничения доступа.

На следующем уровне детализации экран (полупроницаемую мембрану) удобно представлять как последовательность фильтров. Каждый из фильтров, проанализировав данные, может задержать (не пропустить) их, а может и сразу "перебросить" за экран. Кроме того, допускается преобразование данных, передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю (рис. 7).

Рис. 7. Экран как последовательность фильтров.

Помимо функций разграничения доступа, экраны осуществляют протоколирование обмена информацией.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней. Так, межсетевые экраны (МЭ) чаще всего устанавливают для защиты корпоративной сети организации, имеющей выход в Internet.

Экранирование помогает поддерживать доступность сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, вызванную внешней активностью. Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности в ИС организации.

Экранирование может быть частичным, защищающим определенные информационные сервисы (например, экранирование электронной почты).

Ограничивающий интерфейс также можно рассматривать как разновидность экранирования. На невидимый объект трудно нападать, особенно с помощью фиксированного набора средств. В этом смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда гипертекстовые документы формируются динамически. Каждый пользователь видит лишь то, что ему положено видеть. Можно провести аналогию между динамически формируемыми гипертекстовыми документами и представлениями в реляционных базах данных, с той существенной оговоркой, что в случае Web возможности существенно шире.

Экранирующая роль Web-сервиса наглядно проявляется и тогда, когда этот сервис осуществляет посреднические (точнее, интегрирующие) функции при доступе к другим ресурсам, например таблицам базы данных. Здесь не только контролируются потоки запросов, но и скрывается реальная организация данных.

Архитектурные аспекты безопасности

Бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем не представляется возможным. Универсальная ОС - это огромная программа, наверняка содержащая, помимо явных ошибок, некоторые особенности, которые могут быть использованы для нелегального получения привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии учесть все последствия производимых изменений. Наконец, в универсальной многопользовательской системе бреши в безопасности постоянно создаются самими пользователями (слабые и/или редко изменяемые пароли, неудачно установленные права доступа, оставленный без присмотра терминал и т.п.). Единственный перспективный путь связан с разработкой специализированных сервисов безопасности, которые в силу своей простоты допускают формальную или неформальную верификацию. Межсетевой экран как раз и является таким средством, допускающим дальнейшую декомпозицию, связанную с обслуживанием различных сетевых протоколов.

Межсетевой экран располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети). В первом случае говорят о внешнем МЭ, во втором - о внутреннем. В зависимости от точки зрения, внешний межсетевой экран можно считать первой или последней (но никак не единственной) линией обороны. Первой - если смотреть на мир глазами внешнего злоумышленника. Последней - если стремиться к защищенности всех компонентов корпоративной сети и пресечению неправомерных действий внутренних пользователей.

Межсетевой экран - идеальное место для встраивания средств активного аудита. С одной стороны, и на первом, и на последнем защитном рубеже выявление подозрительной активности по-своему важно. С другой стороны, МЭ способен реализовать сколь угодно мощную реакцию на подозрительную активность, вплоть до разрыва связи с внешней средой. Правда, нужно отдавать себе отчет в том, что соединение двух сервисов безопасности в принципе может создать брешь, способствующую атакам на доступность.

На межсетевой экран целесообразно возложить идентификацию/аутентификацию внешних пользователей, нуждающихся в доступе к корпоративным ресурсам (с поддержкой концепции единого входа в сеть).

В силу принципов эшелонированности обороны для защиты внешних подключений обычно используется двухкомпонентное экранирование (см. рис. 8). Первичная фильтрация (например, блокирование пакетов управляющего протокола SNMP, опасного атаками на доступность, или пакетов с определенными IP-адресами, включенными в "черный список") осуществляется граничным маршрутизатором (см. также следующий раздел), за которым располагается так называемая демилитаризованная зона (сеть с умеренным доверием безопасности, куда выносятся внешние информационные сервисы организации - Web, электронная почта и т.п.) и основной МЭ, защищающий внутреннюю часть корпоративной сети.

Теоретически межсетевой экран (особенно внутренний) должен быть многопротокольным, однако на практике доминирование семейства протоколов TCP/IP столь велико, что поддержка других протоколов представляется излишеством, вредным для безопасности (чем сложнее сервис, тем он более уязвим).

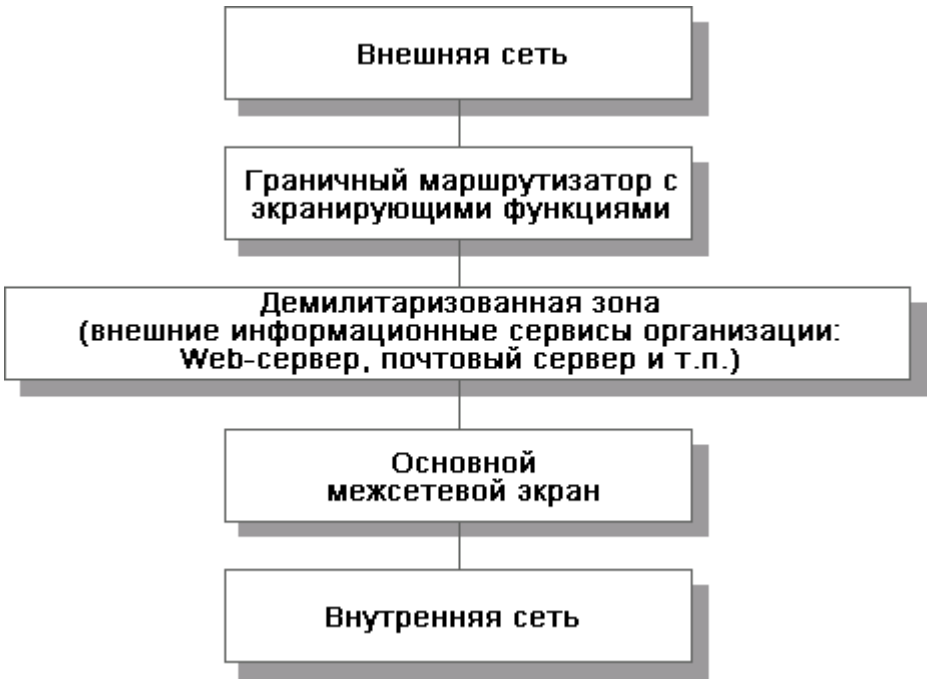

Внешняя сеть
Граничный маршрутизатор с экранирующими функциями
Демилитаризованная зона (внешние информационные сервисы организации: Web-сервер, почтовый сервер и т.п.)
Основной межсетевой экран
Внутренняя сеть

Рис. 8. Двухкомпонентное экранирование с демилитаризованной зоной.

Вообще говоря, и внешний, и внутренний межсетевой экран может стать узким местом, поскольку объем сетевого трафика имеет тенденцию быстрого роста. Один из подходов к решению этой проблемы предполагает разбиение МЭ на несколько аппаратных частей и организацию специализированных серверов-посредников. Основной межсетевой экран может проводить грубую классификацию входящего трафика по видам и передоверять фильтрацию соответствующим посредникам (например, посреднику, анализирующему HTTP-трафик). Исходящий трафик сначала обрабатывается сервером-посредником, который может выполнять и функционально полезные действия, такие как кэширование страниц внешних Web-серверов, что снижает нагрузку на сеть вообще и основной МЭ в частности.

Ситуации, когда корпоративная сеть содержит лишь один внешний канал, являются скорее исключением, чем правилом. Напротив, типична ситуация, при которой корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к Internet. В этом случае каждое подключение должно защищаться своим экраном. Точнее говоря, можно считать, что корпоративный внешний межсетевой экран является составным, и требуется решать задачу согласованного администрирования (управления и аудита) всех компонентов.

Противоположностью составным корпоративным МЭ (или их компонентами) являются персональные межсетевые экраны и персональные экранирующие устройства. Первые являются программными продуктами, которые устанавливаются на персональные компьютеры и защищают только их. Вторые реализуются на отдельных устройствах и защищают небольшую локальную сеть, такую как сеть домашнего офиса.

При развертывании межсетевых экранов следует соблюдать рассмотренные нами ранее принципы архитектурной безопасности, в первую очередь позаботившись о простоте и управляемости, об эшелонированности обороны, а также о невозможности перехода в небезопасное состояние. Кроме того, следует принимать во внимание не только внешние, но и внутренние угрозы.

Системы архивирования и дублирования информации

Организация надежной и эффективной системы архивации данных является одной из важнейших задач по обеспечению сохранности информации в сети. В небольших сетях, где установлены один - два сервера, чаще всего применяется установка системы архивации непосредственно в свободные слоты серверов. В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер.

Такой сервер автоматически производит архивирование информации с жестких дисков серверов и рабочих станций в указанное администратором локальной вычислительной сети время, выдавая отчет о проведенном резервном копировании.

Хранение архивной информации, представляющей особую ценность, должно быть организовано в специальном охраняемом помещении. Специалисты рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании, на случай пожара или стихийного бедствия. Для обеспечения восстановления данных при сбоях магнитных дисков в последнее время чаще всего применяются системы дисковых массивов - группы дисков, работающих как единое устройство, соответствующих стандарту RAID (Redundant Arrays of Inexpensive Disks). Эти массивы обеспечивают наиболее высокую скорость записи/считывания данных, возможность полного восстановления данных и замены вышедших из строя дисков в "горячем" режиме (без отключения остальных дисков массива).

Организация дисковых массивов предусматривает различные технические решения, реализованные на нескольких уровнях:

RAID уровеня 0 предусматривает простое разделение потока данных между двумя или несколькими дисками. Преимущество подобного решения заключается в увеличении скорости ввода/вывода пропорционально количеству задействованных в массиве дисков.

RAID уровня 1 заключается в организации так называемых "зеркальных" дисков. Во время записи данных информация основного диска системы дублируется на зеркальном диске, а при выходе из строя основного диска в работу тут же включается "зеркальный".

RAID уровни 2 и 3 предусматривают создание параллельных дисковых массивов, при записи на которые данные распределяются по дискам на битовом уровне.

RAID уровни 4 и 5 представляют собой модификацию нулевого уровня, при котором поток данных распределяется по дискам массива. Отличие состоит в том, что на уровне 4 выделяется специальный диск для хранения избыточной информации, а на уровне 5 избыточная информация распределяется по всем дискам массива.

Повышение надежности и защита данных в сети, основанная на использовании избыточной информации, реализуются не только на уровне отдельных элементов сети, например дисковых массивов, но и на уровне сетевых ОС. Например, компания Novell реализует отказоустойчивые версии операционной системы Netware - SFT (System Fault Tolerance):

- SFT Level I. Первый уровень предусматривает,создание дополнительных копий FAT и Directory Entries Tables, немедленную верификацию каждого вновь записанного на файловый сервер блока данных, а также резервирование на каждом жестком диске около 2% от объема диска.

- SFT Level II содержала дополнительно возможности создания "зеркальных" дисков, а также дублирования дисковых контроллеров, источников питания и интерфейсных кабелей.

- Версия SFT Level III позволяет использовать в локальной сети дублированные серверы, один из которых является "главным", а второй, содержащий копию всей информации, вступает в работу в случае выхода "главного" сервера из строя.

Анализ защищенности

Сервис анализа защищенности предназначен для выявления уязвимых мест с целью их оперативной ликвидации. Сам по себе этот сервис ни от чего не защищает, но помогает обнаружить (и устранить) пробелы в защите раньше, чем их сможет использовать злоумышленник. В первую очередь, имеются в виду не архитектурные (их ликвидировать сложно), а "оперативные" бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения.

Системы анализа защищенности (называемые также сканерами защищенности), как и рассмотренные выше средства активного аудита, основаны на накоплении и использовании знаний. В данном случае имеются в виду знания о пробелах в защите: о том, как их искать, насколько они серьезны и как их устранять.

Соответственно, ядром таких систем является база уязвимых мест, которая определяет доступный диапазон возможностей и требует практически постоянной актуализации.

В принципе, могут выявляться бреши самой разной природы: наличие вредоносного ПО (в частности, вирусов), слабые пароли пользователей, неудачно сконфигурированные операционные системы, небезопасные сетевые сервисы, неустановленные заплаты, уязвимости в приложениях и т.д. Однако наиболее эффективными являются сетевые сканеры (очевидно, в силу доминирования семейства протоколов TCP/IP), а также антивирусные средства[14]. Антивирусную защиту мы причисляем к средствам анализа защищенности, не считая ее отдельным сервисом безопасности.

---

[14] Биячуев Т.А. Безопасность корпоративных сетей / под ред. Л.Г.Осовецкого. – СПб: СПб ГУ ИТМО, 2004.С.187.

Сканеры могут выявлять уязвимые места как путем пассивного анализа, то есть изучения конфигурационных файлов, задействованных портов и т.п., так и путем имитации действий атакующего. Некоторые найденные уязвимые места могут устраняться автоматически (например, лечение зараженных файлов), о других сообщается администратору.

Контроль, обеспечиваемый системами анализа защищенности, носит реактивный, запаздывающий характер, он не защищает от новых атак, однако следует помнить, что оборона должна быть эшелонированной, и в качестве одного из рубежей контроль защищенности вполне адекватен. Известно, что подавляющее большинство атак носит рутинный характер; они возможны только потому, что известные бреши в защите годами остаются неустраненными.

3. Методы и средства защиты информации в телекоммуникационных сетях предприятия "Вестел"

3.1 Характеристика предприятия и корпоративной сети

Группа компаний Vestel объединяет 19 компаний, специализирующихся на разработке, производстве, маркетинге и дистрибуции бытовой электроники, мелкой и крупной бытовой техники. Являясь одним из лидеров рынка электроники и бытовой техники в Европе, компания имеет представительства в таких странах, как Франция, Испания, Германия, Бельгия, Люксембург, Италия, Великобритания, Голландия, Румыния, Тайвань, Гонконг, Финляндия, США. Производственные и научно-исследовательские мощности также сосредоточены во многих регионах мира. На данный момент Vestel Group входит в крупный транснациональный холдинг Zorlu со штаб-квартирой в городе Стамбул (Турция).

Завод в г. Александров был заложен в ноябре 2002 г., а в ноябре 2003 г. началось производство телевизоров. В 2006 году был построен цех по производству стиральных машин и холодильников. На данный момент на российском рынке представлены кинескопные, жидкокристаллические и плазменные телевизоры, стиральные машины, холодильники, плиты. На заводе применяются самые современные сборочные технологии и полностью автоматизированные системы контроля качества.

Число работающих – более 700 человек (около 500 из них – рабочие).

На предприятии отсутствуют сведения, составляющие государственную тайну, но ведется работа с коммерческой и служебной тайной.

На предприятии существует своя локальная сеть, доступ к которой имеют только работники Вестела. В большинстве случаев имеется доступ лишь к ограниченному числу сайтов этой сети, необходимых в ходе трудовой деятельности. Информация о каждом выходе в сеть фиксируется системным администратором. Это также относится к сети Интернет.

Количество рабочих станций в сети – 27. Они объединены в несколько рабочих групп:

директор предприятия – 1 рабочая станция;

отдел №1 - 2 рабочих станции;

секретарь – 1 рабочая станция;

отделения 1, 2 и 3 отдела №2 по 3, 2 и 4 рабочих станции соответственно;

отделения 4 и 5 отдела №3 по 3 и 4 рабочих станции;

отделение 6 отдела №4 – 3 рабочих станции;

отдел №5 – 4 рабочие станции;

отдел №6 – 4 рабочие станции.

Вся сеть расположена на одном этаже административного здания.

План помещений, где расположены рабочие станции и сервер представлен в Приложении Б.

Сеть, как это видно из рис. 9, имеет топологию «звезда».

Топология типа «звезда» представляет собой более производительную структуру, каждый компьютер, в том числе и сервер, соединяется отдельным сегментом кабеля с центральным концентратором (HAB).

Основным преимуществом такой сети является её устойчивость к сбоям, возникающим вследствие неполадок на отдельных ПК или из-за повреждения сетевого кабеля. [7]

Используемый метод доступа - CSMA/CD. Именно этот метод доступа применяет сетевая архитектура Ethernet, которая используется на предприятии. Сеть построена на основе на основе витой пары (10Base – T) с использованием кабеля фирмы Siemon, стандарта UTP (Unshielded Twisted Pair) (неэкранированная витая пара) категории 5, международного стандарта Кабельных систем.

Используемые операционные системы - Windows 2000 (на рабочих станциях) и Windows 2003 Server.

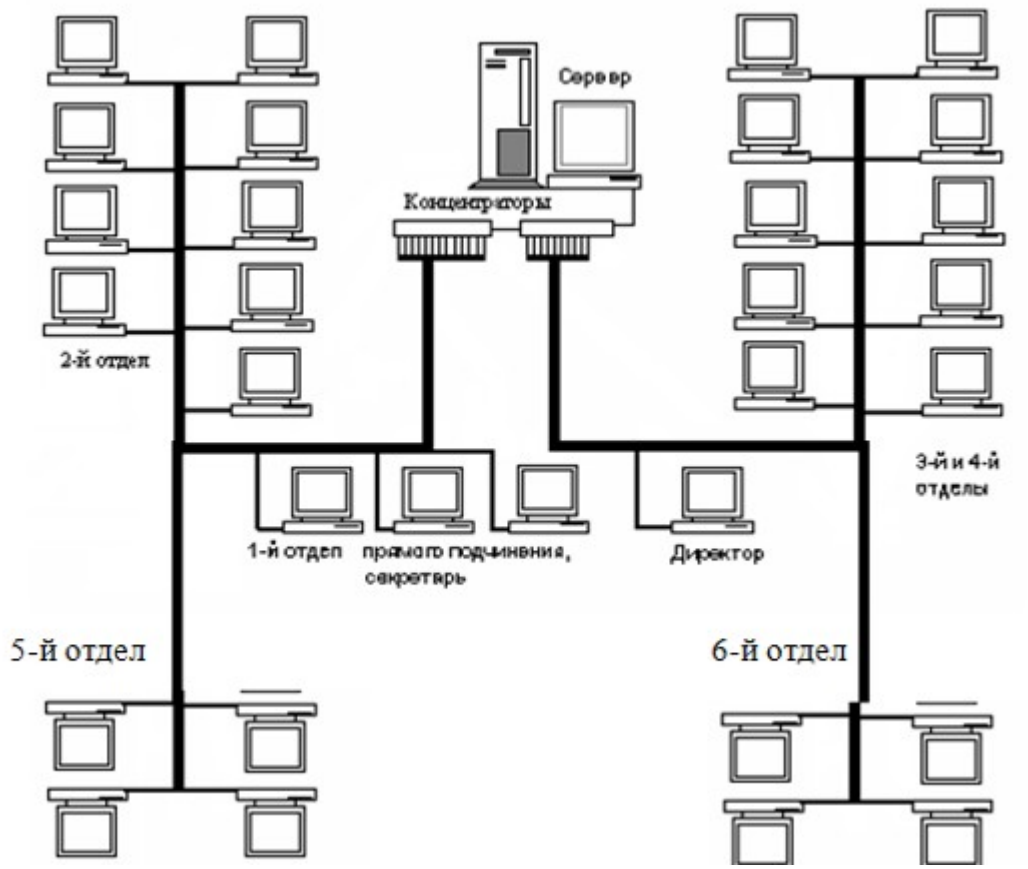


Рис. 9. Топология сети предприятия.

3.2 Организационно-правовое обеспечение защиты информации

На предприятии разработаны следующие меры по защите информации:

— заключен договор об охране помещения и территории (действует пропускной режим);

— разработан режим и правила противопожарной безопасности;

— режим видеонаблюдения этажей;

— разработаны должностные инструкции служащих, разграничивающие их права и обязанности;

—дополнительные соглашения к трудовым договорам сотрудников о неразглашении ими конфиденциальной информации, регламентирующие ответственность в области защиты информации;

— инструкции по охране периметра, по эксплуатации системы охранной сигнализации и видеонаблюдения;

— положение о конфиденциальном документообороте;

— описание технологического процесса обработки КИ;

— установлена антивирусная системы защиты на АРМ;

— разграничен доступ к АРМ паролями.

Правовое обеспечение системы защиты конфиденциальной информации включает в себя комплекс внутренней нормативно-организационной документации, в которую входят такие документы предприятия, как:

- Устав;

- коллективный трудовой договор;

- трудовые договоры с сотрудниками предприятия;

- правила внутреннего распорядка служащих предприятия;

- должностные обязанности руководителей, специалистов и служащих предприятия.

- инструкции пользователей информационно-вычислительных сетей и баз данных;

- инструкции сотрудников, ответственных за защиту информации;

- памятка сотрудника о сохранении коммерческой или иной тайны;

- договорные обязательства.

Не углубляясь в содержание перечисленных документов, можно сказать, что во всех из них, в зависимости от их основного нормативного или юридического назначения, указываются требования, нормы или правила по обеспечению необходимого уровня информационной защищенности предприятия, обращенные, прежде всего, к персоналу и руководству.

Правовое обеспечение дает возможность урегулировать многие спорные вопросы, неизбежно возникающие в процессе информационного обмена на самых разных уровнях - от речевого общения до передачи данных в компьютерных сетях. Кроме того, образуется юридически оформленная система административных мер, позволяющая применять взыскания или санкции к нарушителям внутренней политики безопасности, а также устанавливать достаточно четкие условия по обеспечению конфиденциальности сведений, используемых или формируемых при сотрудничестве между субъектами экономики, выполнении ими договорных обязательств, осуществлении совместной деятельности и т.п. При этом стороны, не выполняющие эти условия, несут ответственность в рамках, предусмотренных как соответствующими пунктами меж сторонних документов (договоров, соглашений, контрактов и пр.), так и российским законодательством.

Основными объектами защиты являются:

— АРМ сотрудников;

— сервер локальной сети;

— конфиденциальная информация (документы);

— кабинеты генерального директора, главного инженера и главного технолога;

— кабинеты с конфиденциальной документацией.

3.3 Защита информации в корпоративной сети «Вестел» на уровне операционной системы

Windows 2003 Server имеет средства обеспечения безопасности, встроенные в операционную систему. Ниже рассмотрены наиболее значимые из них.

Слежение за деятельностью сети.

Windows 2003 Server дает много инструментальных средств для слежения за сетевой деятельностью и использованием сети. ОС позволяет:

просмотреть сервер и увидеть, какие ресурсы он использует;

увидеть пользователей, подключенных в настоящее время к серверу и увидеть, какие файлы у них открыты;

проверить данные в журнале безопасности;

проверитьзаписи в журнале событий;

указать, о каких ошибках администратор должен быть предупрежден, если они произойдут.

Начало сеанса на рабочей станции

Всякий раз, когда пользователь начинает сеанс на рабочей станции, экран начала сеанса запрашивает имя пользователя, пароль и домен. Затем рабочая станция посылает имя пользователя и пароль в домен для идентификации. Сервер в домене проверяет имя пользователя и пароль в базе данных учетных карточек пользователей домена. Если имя пользователя и пароль идентичны данным в учетной карточке, сервер уведомляет рабочую станцию о начале сеанса. Сервер также загружает другую информацию при начале сеанса пользователя, как например установки пользователя, свой каталог и переменные среды.

По умолчанию не все учетные карточки в домене позволяют входить в систему. Только карточкам групп администраторов, операторов сервера, операторов управления печатью, операторов управления учетными карточками и операторов управления резервным копированием разрешено это делать.

Для всех пользователей сети предприятия предусмотрено свое имя и пароль (подробнее об этом рассказывается в следующем разделе ВКР).

Учетные карточки пользователей

Каждый клиент, который использует сеть, имеет учетную карточку пользователя в домене сети. Учетная карточка пользователя содержит информацию о пользователе, включающую имя, пароль и ограничения по использованию сети, налагаемые на него. Учетные карточки позволяют сгруппировать пользователей, которые имеют аналогичные ресурсы, в группы; группы облегчают предоставление прав и разрешений на ресурсы, достаточно сделать только одно действие, дающее права или разрешения всей группе.

Приложение В показывает содержимое учетной карточки пользователя.

Журнал событий безопасности

Windows 2003 Server позволяет определить, что войдет в ревизию и будет записано в журнал событий безопасности всякий раз, когда выполняются определенные действия или осуществляется доступ к файлам. Элемент ревизии показывает выполненное действие, пользователя, который выполнил его, а также дату и время действия. Это позволяет контролировать как успешные, так и неудачные попытки каких-либо действий.

Журнал событий безопасности для условий предприятия является обязательным, так как в случае попытки взлома сети можно будет отследить источник.

На самом деле протоколирование осуществляется только в отношении подозрительных пользователей и событий. Поскольку если фиксировать все события, объем регистрационной информации, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. Слежка важна в первую очередь как профилактическое средство. Можно надеяться, что многие воздержатся от нарушений безопасности, зная, что их действия фиксируются.

Права пользователя

Права пользователя определяют разрешенные типы действий для этого пользователя. Действия, регулируемые правами, включают вход в систему на локальный компьютер, выключение, установку времени, копирование и восстановление файлов сервера и выполнение других задач.

В домене Windows 2003 Server права предоставляются и ограничиваются на уровне домена; если группа находится непосредственно в домене, участники имеют права во всех первичных и резервных контроллерах домена.

Для каждого пользователя предприятия обязательно устанавливаются свои права доступа к информации, разрешение на копирование и восстановление файлов.

Установка пароля и политика учетных карточек

Для домена определены все аспекты политики пароля: минимальная длина пароля (6 символов), минимальный и максимальный возраст пароля и исключительность пароля, который предохраняет пользователя от изменения его пароля на тот пароль, который пользователь использовал недавно.

Дается возможность также определить и другие аспекты политики учетных карточек:

- должна ли происходить блокировка учетной карточки;

- должны ли пользователи насильно отключаться от сервера по истечении часов начала сеанса;

- должны ли пользователи иметь возможность входа в систему, чтобы изменить свой пароль.

Когда разрешена блокировка учетной карточки, тогда учетная карточка блокируется в случае нескольких безуспешных попыток начала сеанса пользователя, и не более, чем через определенный период времени между любыми двумя безуспешными попытками начала сеанса. Учетные карточки, которые заблокированы, не могут быть использованы для входа в систему.

Если пользователи принудительно отключаются от серверов, когда время его сеанса истекло, то они получают предупреждение как раз перед концом установленного периода сеанса. Если пользователи не отключаются от сети, то сервер произведет отключение принудительно. Однако отключения пользователя от рабочей станции не произойдет. Часы сеанса на предприятии не установлены, так как в успешной деятельности заинтересованы все сотрудники и зачастую некоторые остаются работать сверхурочно или в выходные дни.

Если от пользователя требуется изменить пароль, то, когда он этого не сделал при просроченном пароле, он не сможет изменить свой пароль. При просрочке пароля пользователь должен обратиться к администратору системы за помощью в изменении пароля, чтобы иметь возможность снова входить в сеть. Если пользователь не входил в систему, а время изменения пароля подошло, то он будет предупрежден о необходимости изменения, как только он будет входить.

Шифрованная файловая система EFS

Windows 2000 предоставляет возможность еще больше защитить зашифрованные файлы и папки на томах NTFS благодаря использованию шифрованной файловой системы EFS (Encrypting File System). При работе в среде Windows 2000 можно работать только с теми томами, на которые есть права доступа.

При использовании шифрованной файловой системы EFS можно файлы и папки, данные которых будут зашифрованы с помощью пары ключей. Любой пользователь, который захочет получить доступ к определенному файлу, должен обладать личным ключом, с помощью которого данные файла будут расшифровываться. Система EFS так же обеспечивает схему защиты файлов в среде Windows 2000. Однако, на предприятии не используется эта возможность, так как при использовании шифрования производительность работы системы снижается.

3.4 Защита информации от несанкционированного доступа

Выше уже были указаны организационно-правовые аспекты защиты информации от несанкционированного доступа и возможности Windows 2000 в этом плане. Теперь остановлюсь чуть подробнее на других аспектах.

Информация, циркулирующая в корпоративной сети весьма разнообразна. Все информационные ресурсы разделены на три группы:

Сетевые ресурсы общего доступа;

Информационные ресурсы файлового сервера;

Информационные ресурсы СУБД.

Каждая группа содержит ряд наименований информационных ресурсов, которые в свою очередь имеют индивидуальный код, уровень доступа, расположение в сети, владельца и т.п.

Эта информация важна для предприятия и его клиентов, поэтому она должна иметь хорошую защиту.

Электронные ключи

Все компьютеры, работающие со сведениями, составляющими коммерческую тайну, оборудованы дополнительными программно-аппаратными комплексами.

Такие комплексы представляют собой совокупность программных и аппаратных средств защиты информации от несанкционированного доступа.

Аппаратная часть, подобных комплексов так называемый электронный замок представляет собой электронную плату, вставляемую в один из слотов компьютера и снабженную интерфейсом для подключения считывателя электронных ключей таких типов как: Smart Card, Touch Memory, Proximity Card, eToken. Типичным набором функций, предоставляемых такими электронными замками, является:

- регистрации пользователей компьютера и назначения им персональных идентификаторов (имен и/или электронных ключей) и паролей для входа в систему;

- запрос персонального идентификатора и пароля пользователя при загрузке компьютера. Запрос осуществляется аппаратной частью до загрузки ОС;

- возможность блокирования входа в систему зарегистрированного пользователя;

- ведение системного журнала, в котором регистрируются события, имеющие отношение к безопасности системы;

- контроль целостности файлов на жестком диске;

- контроль целостности физических секторов жесткого диска;

- аппаратную защиту от несанкционированной загрузки операционной системы с гибкого диска,CD-ROM или USB портов;

- возможность совместной работы с программными средствами защиты от несанкционированного доступа.

Попечительская защита данных

На предприятии используется такой вариант защиты информации как попечительская защита данных. Попечитель - это пользователь, которому предоставлены привилегии или права доступа к файловым информационным ресурсам.

Каждый сотрудник имеет одну из восьми разновидностей прав:

Read - право Чтения открытых файлов;

Write - право Записи в открытые файлы;

Open - право Открытия существующего файла;

Create - право Создания (и одновременно открытия) новых файлов;

Delete - право Удаления существующих файлов;

Parental - Родительские права:

- право Создания, Переименования, Стирания подкаталогов каталога;

- право Установления попечителей и прав в каталоге;

- право Установления попечителей и прав в подкаталоге;

Search - право Поиска каталога;

Modify - право Модификации файловых атрибутов.

Для предотвращения случайных изменений или удаления отдельных файлов всеми работниками используется защита атрибутами файлов. Такая защита применяется в отношении информационных файлов общего пользования, которые обычно читаются многими пользователями. В защите данных используются четыре файловых атрибута:

Запись-чтение,

Только чтение,

Разделяемый,

Неразделяемый.

Пароли

Как я уже указывал, все компьютеры на предприятии защищены с помощью паролей.

Поскольку на всех компьютерах организации установлен Microsoft Windows 2000 и Windows Server 2003, то используется защита паролем операционной системы, которая устанавливается администратором в BIOS, так как важнейшую роль в предотвращении несанкционированного доступа к данным компьютера играет именно защита BIOS.

Модификация, уничтожение BIOS персонального компьютера возможно в результате несанкционированного сброса или работы вредоносных программ, вирусов.

В зависимости от модели компьютера защита BIOS обеспечивается:

- установкой переключателя, расположенного на материнской плате, в положение, исключающее модификацию BIOS (производится службой технической поддержки подразделения автоматизации);

- установкой административного пароля в ПО SETUP.

Защита BIOS от несанкционированного сброса обеспечивается опечатыванием корпуса компьютера защитной голографической наклейкой.

Используются два типа паролей доступа: административные и пользовательские.

При установке административного и пользовательского паролей следует руководствоваться следующими правилами:

- пользовательский пароль пользователь компьютера выбирает и вводит единолично (не менее 6-ти символов). Администратору информационной безопасности запрещается узнавать пароль пользователя.

- административный пароль (не менее 8-ми символов) вводится администратором информационной безопасности. Администратору информационной безопасности запрещается сообщать административный пароль пользователю.

В том случае если компьютер оборудован аппаратно-программным средством защиты от НСД, которое запрещает загрузку ОС без предъявления пользовательского персонального идентификатора, пользовательский пароль допускается не устанавливать.

При положительном результате проверки достоверности предъявленного пользователем пароля:

- система управления доступом предоставляет пользователю закрепленные за ним права доступа;

- пользователь регистрируется встроенными средствами регистрации (если они имеются).

Контроль доступа в Интернет

Особое внимание следует уделять доступу работников предприятия к сети Интернет.

Раньше доступ к сети Internet осуществлялся со специализированного рабочего места, называемого Интернет-киоском. Интернет-киоск не был подключен к корпоративной сети предприятия.

В подразделении, осуществлявшем эксплуатацию Интернет-киоска, велись:

- журнал учета работ в сети Internet, в котором отражались: ФИО пользователя, дата, время начала работ, продолжительность работ, цель работ, используемые ресурсы, подпись;

- журнал допуска, в котором отражались: ФИО пользователя, задачи, для решения которых он допускается к работе в сети Internet, время проведения работ и максимальная продолжительность, подпись руководителя.

Но от этой практики впоследствии отказались. Сейчас все компьютеры корпоративной сети имеют выход в Интернет.

Рост спектра и объемов услуг, влекущие за собой потребность подразделений в информационном обмене с внешними организациями, а также необходимость предоставления удаленного доступа к информации через публичные каналы связи, значительно повышают риски несанкционированного доступа, вирусной атаки и т.п.

3.5 Антивирусная защита

Учитываемые факторы риска

Вирусы могут проникать в машину различными путями (через глобальную сеть, через зараженную дискету или флешку). Последствия их проникновения весьма неприятны: от разрушения файла до нарушения работоспособности всего компьютера. Достаточно всего лишь одного зараженного файла, чтобы заразить всю имеющуюся на компьютере информацию, а далее заразить всю корпоративную сеть.

При организации системы антивирусной защиты на предприятии учитывались следующие факторы риска:

- ограниченные возможности антивирусных программ

Возможность создания новых вирусов с ориентацией на противодействие конкретным антивирусным пакетам и механизмам защиты, использование уязвимостей системного и прикладного ПО приводят к тому, что даже тотальное применение антивирусных средств с актуальными антивирусными базами не дает гарантированной защиты от угрозы вирусного заражения, поскольку возможно появление вируса, процедуры защиты от которого еще не добавлены в новейшие антивирусные базы.

- высокая интенсивность обнаружения критичных уязвимостей в системном ПО

Наличие новых неустраненных критичных уязвимостей в системном ПО, создает каналы массового распространения новых вирусов по локальным и глобальным сетям. Включение в состав вирусов «троянских» модулей, обеспечивающих возможность удаленного управления компьютером с максимальными привилегиями, создает не только риски массового отказа в обслуживании, но и риски прямых хищений путем несанкционированного доступа в автоматизированные банковские системы.

- необходимость предварительного тестирования обновлений системного и антивирусного ПО

Установка обновлений без предварительного тестирования создает риски несовместимости системного, прикладного и антивирусного ПО и может приводить к нарушениям в работе. В то же время тестирование приводит к дополнительным задержкам в установке обновлений и соответственно увеличивает риски вирусного заражения.

- разнообразие и многоплатформенность используемых в автоматизированных системах технических средств и программного обеспечения

Возможность работы отдельных типов вирусов на различных платформах, способность вирусов к размножению с использованием корпоративных почтовых систем или вычислительных сетей, отсутствие антивирусных продуктов для некоторых конкретных платформ делают в ряде случаев невозможным или неэффективным применение антивирусного ПО.

- широкая доступность современных мобильных средств связи, устройств хранения и носителей информации большой емкости

Современные мобильные средства связи позволяют недобросовестным сотрудникам произвести несанкционированное подключение автоматизированного рабочего места к сети Интернет, создав тем самым брешь в периметре безопасности корпоративной сети и подвергнув ее информационные ресурсы риску массового заражения новым компьютерным вирусом. Наличие доступных компактных устройств хранения и переноса больших объемов информации создает условия для несанкционированного использования таких устройств и носителей в личных, не производственных целях. Несанкционированное копирование на компьютеры предприятия информации, полученной из непроверенных источников, существенно увеличивает риски вирусного заражения.

- необходимость квалифицированных действий по отражению вирусной атаки

Неквалифицированные действия по отражению вирусной атаки могут приводить к усугублению последствий заражения, частичной или полной утрате критичной информации, неполной ликвидации вирусного заражения или даже расширению очага заражения.

- необходимость планирования мероприятий по выявлению последствий вирусной атаки и восстановлению пораженной информационной системы

В случае непосредственного воздействия вируса на автоматизированную банковскую систему, либо при проведении неквалифицированных лечебных мероприятий может быть утрачена информация или искажено программное обеспечение.

В условиях действия указанных факторов только принятие жестких комплексных мер безопасности по всем возможным видам угроз позволит контролировать постоянно растущие риски полной или частичной остановки бизнес процессов в результате вирусных заражений.

Пакет Dr.Web

Для антивирусной защиты был выбран пакет Dr.Web Enterprise Suite. Этот пакет обеспечивает централизованную защиту корпоративной сети любого масштаба. Современное решение на базе технологий Dr.Web для корпоративных сетей, представляет собой уникальный технический комплекс со встроенной системой централизованного управления антивирусной защитой в масштабе предприятия. Dr.Web Enterprise Suite позволяет администратору, работающему как внутри сети, так и на удаленном компьютере (через сеть Internet) осуществлять необходимые административные задачи по управлению антивирусной защитой организации.

Основные возможности:

Быстрое и эффективное распространение сервером Dr.Web Enterprise Suite обновлений вирусных баз и программных модулей на защищаемые рабочие станции.

Минимальный, в сравнении с аналогичными решениями других производителей, сетевой трафик построенных на основе протоколов IP, IPX и NetBIOS с возможностью применения специальных алгоритмов сжатия.

Возможность установки рабочего места администратора (консоли управления антивирусной защитой) практически на любом компьютере под управлением любой операционной системы.

Ключевой файл клиентского ПО и сервера, по умолчанию, хранится на сервере.

Сканер Dr.Web с графическим интерфейсом. Сканирует выбранные пользователем объекты на дисках по требованию, обнаруживает и нейтрализует вирусы в памяти, проверяет файлы автозагрузки и процессы.

Резидентный сторож (монитор) SpIDer Guard. Контролирует в режиме реального времени все обращения к файлам, выявляет и блокирует подозрительные действия программ.

Резидентный почтовый фильтр SpIDer Mail. Контролирует в режиме реального времени все почтовые сообщения, входящие по протоколу POP3 и исходящие по протоколу SMTP. Кроме того, обеспечивает безопасную работу по протоколам IMAP4 и NNTP.

Консольный сканер Dr.Web. Сканирует выбранные пользователем объекты на дисках по требованию, обнаруживает и нейтрализует вирусы в памяти, проверяет файлы автозагрузки и процессы.

Утилита автоматического обновления. Загружает обновления вирусных баз и программных модулей, а также осуществляет процедуру регистрации и доставки лицензионного или демонстрационного ключевого файла.

Планировщик заданий. Позволяет планировать регулярные действия, необходимые для обеспечения антивирусной защиты, например, обновления вирусных баз, сканирование дисков компьютера, проверку файлов автозагрузки.

Dr.Web для Windows 5.0 обеспечивает возможность лечения активного заражения, включает технологии обработки процессов в памяти и отличается вирусоустойчивостью. В частности, Dr.Web способен обезвреживать сложные вирусы, такие как MaosBoot, Rustock.C, Sector. Как отмечается, технологии, позволяющие Dr.Web эффективно бороться с активными вирусами, а не просто детектировать лабораторные коллекции, получили в новой версии свое дальнейшее развитие.

В модуле самозащиты Dr.Web SelfProtect ведется полноценный контроль доступа и изменения файлов, процессов, окон и ключей реестра приложения. Сам модуль самозащиты устанавливается в систему в качестве драйвера, выгрузка и несанкционированная остановка работы которого невозможны до перезагрузки системы.

В версии 5.0 реализована новая технология универсальной распаковки Fly-code, которая позволяет детектировать вирусы, скрытые под неизвестными Dr.Web упаковщиками, базируясь на специальных записях в вирусной базе Dr.Web и эвристических предположениях поискового модуля Dr.Web о возможно содержащемся в упакованном архиве вредоносном объекте.

Противостоять неизвестным угрозам Dr.Web также помогает и технология несигнатурного поиска Origins Tracing, получившая в новой версии свое дальнейшее развитие. Как утверждают разработчики, Origins Tracing дополняет традиционные сигнатурный поиск и эвристический анализатор Dr.Web и повышает уровень детектирования ранее неизвестных вредоносных программ.

Кроме того, по данным «Доктор Веб», Dr.Web для Windows способен не только детектировать, но и эффективно нейтрализовать вирусы, использующие руткит-технологии. В версии 5.0 реализована принципиально новая версия драйвера Dr.Web Shield, которая позволяет бороться даже с руткит-технологиями будущего поколения. В то же время, Dr.Web способен полностью проверять архивы любого уровня вложенности. Помимо работы с архивами, в Dr.Web для Windows версии 5.0 добавлена поддержка десятков новых упаковщиков и проведен ряд улучшений при работе с упакованными файлами, в том числе файлами, упакованными многократно и даже разными упаковщиками.

За счет включения новых и оптимизации существующих технологий Dr.Web для Windows разработчикам удалось ускорить процесс сканирования. Благодаря возросшему быстродействию антивирусного ядра, сканер Dr.Web на 30% быстрее предыдущей версии проверяет оперативную память, загрузочные секторы, содержимое жестких дисков и сменных носителей, утверждают в компании.

Среди новинок можно отметить HTTP-монитор SpIDer Gate. HTTP-монитор SpIDer Gate проверяет весь входящий и исходящий HTTP-трафик, при этом совместим со всеми известными браузерами, и его работа практически не сказывается на производительности ПК, скорости работы в интернете и количестве передаваемых данных. Фильтруются все данные, поступающие из интернета — файлы, аплеты, скрипты, что позволяет скачивать на компьютер только проверенный контент.

Тестирование пакета Dr.Web

Чтобы удостовериться, что выбранный в качестве корпоративного антивирусного пакета Dr.Web является действительно надежным средством, я изучил несколько обзоров антивирусных программ и ознакомился с несколькими результатами тестов.

Результаты теста по вероятностной методике (сайт antivirus.ru) отдают Dr.Web первое место (Приложение Г).

По результатам февральского тестирования антивирусных программ, проведенного журналом Virus Bulletin, отечественный полифаг Dr. Web занял 8-е место среди лучших антивирусов в мире. Программа Dr. Web показала абсолютный результат 100% в важной и престижной (технологической) категории - по степени обнаружения сложных полиморфных вирусов. Следует особо отметить, что в тестах журнала Virus Bulletin 100%-го результата по обнаружению полиморфных вирусов программа Dr. Web стабильно добивается (январь 2007, июль-август 2007 и январь 2008) уже третий раз подряд. Такой стабильностью по этой категории не может похвастаться ни один другой антивирусный сканер.

Высочайший уровень в 100% достигнут программой Dr. Web также и в очень актуальной категории - по обнаружению макро-вирусов.

Заключение

Прогресс подарил человечеству великое множество достижений, но тот же прогресс породил и массу проблем. Человеческий разум, разрешая одни проблемы, непременно сталкивается при этом с другими, новыми. Вечная проблема - защита информации. На различных этапах своего развития человечество решало эту проблему с присущей для данной эпохи характерностью. Изобретение компьютера и дальнейшее бурное развитие информационных технологий во второй половине 20 века сделали проблему защиты информации настолько актуальной и острой, насколько актуальна сегодня информатизация для всего общества. Главная тенденция, характеризующая развитие современных информационных технологий - рост числа компьютерных преступлений и связанных с ними хищений конфиденциальной и иной информации, а также материальных потерь.

Сегодня, наверное, никто не сможет с уверенностью назвать точную цифру суммарных потерь от компьютерных преступлений, связанных с несанкционированных доступом к информации. Это объясняется, прежде всего, нежеланием пострадавших компаний обнародовать информацию о своих потерях, а также тем, что не всегда потери от хищения информации можно точно оценить в денежном эквиваленте.

Причин активизации компьютерных преступлений и связанных с ними финансовых потерь достаточно много, существенными из них являются:

- переход от традиционной "бумажной" технологии хранения и передачи сведений на электронную и недостаточное при этом развитие технологии защиты информации в таких технологиях;

- объединение вычислительных систем, создание глобальных сетей и расширение доступа к информационным ресурсам;

- увеличение сложности программных средств и связанное с этим уменьшение их надежности и увеличением числа уязвимостей.

Компьютерные сети, в силу своей специфики, просто не смогут нормально функционировать и развиваться, игнорируя проблемы защиты информации.

В первой главе моей квалификационной работы были рассмотрены различные виды угроз и рисков. Угрозы безопасности делятся не естественные и искусственные, а искусственные в свою очередь делятся на непреднамеренные и преднамеренные.

К самым распространенным угрозам относятся ошибки пользователей компьютерной сети, внутренние отказы сети или поддерживающей ее инфраструктуры, программные атаки и вредоносное программное обеспечение.

Меры обеспечения безопасности компьютерных сетей подразделяются на: правовые (законодательные), морально-этические, организационные (административные), физические, технические (аппаратно-программные).

Во второй главе ВКР я подробно рассмотрел некоторые из физических, аппаратных и программных способов защиты. К современным программным средствам защиты информации относятся криптографические методы, шифрование дисков, идентификация и аутентификация пользователя. Для защиты локальной или корпоративной сети от атак из глобальной сети применяют специализированные программные средства: брэндмауэры или прокси-серверы. Брэндмауэры – это специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/ транспортного уровней. Прокси-сервер – это сервер-посредник, все обращения из локальной сети в глобальную происходят через него.

Организация надежной и эффективной системы архивации данных также является одной из важнейших задач по обеспечению сохранности информации в сети. Для обеспечения восстановления данных при сбоях магнитных дисков в последнее время чаще всего применяются системы дисковых массивов - группы дисков, работающих как единое устройство, соответствующих стандарту RAID.

Для выявления уязвимых мест с целью их оперативной ликвидации предназначен сервис анализа защищенности. Системы анализа защищенности (называемые также сканерами защищенности), как и рассмотренные выше средства активного аудита, основаны на накоплении и использовании знаний. В данном случае имеются в виду знания о пробелах в защите: о том, как их искать, насколько они серьезны и как их устранять.

В третьей главе ВКР мною рассмотрены методы и средства защиты информации в телекоммуникационных сетях предприятия Вестел. Кратко описав предприятие и его корпоративную сеть, я остановился на организационно-правовом обеспечении защиты, подробно рассмотрел защитные возможности операционной системы Windows 2003 Server, используемой на предприятии. Очень важно защитить корпоративную сеть от несанкционированного доступа. Для этого на предприятии используются электронные ключи, организована попечительская защита данных, установлены пароли, осуществляется контроль доступа в Интернет.

Чтобы исключить заражение корпоративной сети компьютерными вирусами, Вестел использует пакет антивирусных программ Dr.Web Enterprise Suite. Преимуществами этого пакета являются:

Масштабируемость;

Единый центр управления;

Низкозатратное администрирование;

Экономия трафика локальной сети;

Широкий спектр поддержки протоколов.

К этому следует добавить привлекательность цены.

Чтобы удостовериться, что выбранный в качестве корпоративного антивирусного пакета Dr.Web является лучшим решением, я изучил несколько обзоров антивирусных программ и ознакомился с результатами нескольких тестов. Результаты теста по вероятностной методике (сайт antivirus.ru) отдают Dr.Web первое место, а журнал Virus Bulletin ставит Dr. Web на 8-е место среди лучших антивирусов в мире.

Проанализировав доступную мне информацию об организации защиты корпоративной сети Вестела, я сделал следующий вывод:

Вестел это крупное предприятие со своей четко организованной системой безопасности. Специалисты предприятия создали грамотную и надежно работающую систему защиты. Мне сложно что-либо предлагать для усовершенствования ее технологий. Разумеется, можно выделить наиболее действенные меры защиты информации в сетях это:

- разграничение полномочий;
- использование лицензионного ПО;
- идентификация и аутентификация пользователей;
- резервное копирование;
- хорошее антивирусное программное обеспечение;
- регулярное обновление антивирусной базы.

В этом случае степень защиты информации значительно возрастет.

Глоссарий

№	Понятие	Содержание
1	Абонент сети	лицо, являющееся сотрудником учреждения (предприятия), имеющее соответствующим образом оформленное разрешение и технические возможности на подключение и взаимодействие с Сетями.
2	Блокирование компьютерной информации	физическое воздействие на компьютерную информацию, ее машинный носитель и (или) программно-технические средства ее обработки и защиты, результатом которого явилась временная или постоянная невозможность осуществлять какие-либо операции над компьютерной информацией.
3	Вредоносная программа для ЭВМ	программа для ЭВМ, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети без предварительного предупреждения пользователя о характере действия программы и не запрашивающая его разрешения на реализацию программой своего назначения.
4	Достоверность передачи информации	соответствие принятого сообщения переданному. Определяет степень вероятности отсутствия ошибок в полученном сообщении.
5	Зашифрованный диск	файл-контейнер, внутри которого могут находиться любые другие файлы или программы (они могут быть установлены и запущены прямо из этого зашифрованного файла)
6	Категорирование защищаемой информации (объекта защиты)	установление градаций важности защиты защищаемой информации (объекта защиты).
7	Компьютерный вирус	фрагмент исполняемого кода, который копирует себя в другую программу (главную программу), модифицируя ее при этом. Дублируя себя, вирус заражает другие программы. Вирус выполняется только при запуске главной программы и вызывает ее непредсказуемое поведение, приводящее к уничтожению и искажению данных и программ
8	Криптография	специальная система изменения открытого письма с целью сделать текст понятным лишь для тех лиц, которые знают эту систему; тайнопись (от греч. "криптос" - скрытый и "графо" - пишу).

9	Криптографический протокол	совокупностью действий (инструкций, команд, вычислений, алгоритмов), выполняемых в заданной последовательности двумя или более объектами (субъектами) криптографической системы для достижения следующих целей: обмена ключевой информацией с последующей установкой засекреченного режима передачи и приема сообщений; аутентификации; авторизации. Субъекты криптографической системы - это люди (пользователи), а объекты - автоматы (технические устройства).
10	Межсетевой экран (МЭ)	это локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в КС и/или выходящей из КС. МЭ обеспечивает защиту КС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в/из КС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной КС к объектам другой КС.
11	Нарушение безопасности информации	событие, при котором компрометируется один или несколько аспектов безопасности информации (доступность, конфиденциальность, целостность и достоверность)
12	Пароль	секретная строка символов, предъявляемая пользователем компьютерной системе для получения доступа к данным и программам. Пароль является средством защиты данных от несанкционированного доступа
13	Правило доступа к информации	правило доступа: совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.
14	Технический канал утечки информации	совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.
15	Файловый вирус	компьютерный вирус, прикрепляющий себя к файлу или программе, и активизирующийся при каждом использовании файла
16	Электронное сообщение	информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Список использованных источников

1. Андреев Б. В. Защита прав и свобод человека и гражданина в информационной сфере // Системы безопасности, № 1, 2002. С. 10–13
2. Байбурин В.Б., Бровкова М.Б., Пластун И.Л., Мантуров А.О., Данилова Т.В., Макарцова Е.А. Введение в защиту информации. Учебное пособие (Серия "Профессиональное образование"), (ГРИФ). - М.:"Инфра-М", 2004. - 128 с.
3. Балдин В.К., Уткин В.Б. Информатика: Учеб. для вузов. - М.: Проект, 2003. - 304 с.
4. Бармен С. Разработка правил информационной безопасности. - М.: Издательский дом "Вильямс", 2002. - 208 с.
5. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право.– Спб.: Изд-во «Юридический центр Пресс», 2001.
6. Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие / под ред. Л.Г.Осовецкого - СПб.: СПбГУ ИТМО, 2004. - 161 с.
7. Блэк У. Интернет: протоколы безопасности. Учебный курс. - СПб.: Питер, 2001. - 288 с.: ил.
8. Бождай А.С., Финогеев А.Г. Сетевые технологии. Часть 1: Учебное пособие. - Пенза: Изд-во ПГУ, 2005. - 107 с.
9. Бэнкс М. Информационная защита ПК (с CD-ROM). - Киев: "Век", 2001. - 272 с.
10. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. - М.: Московский центр непрерывного математического образования, 2003. - 328 с.
11. Вихорев С. В., Кобцев Р. Ю. Как узнать – откуда напасть или откуда исходит угроза безопасности информации // Защита информации. Конфидент, № 2, 2002.
12. Вычислительные системы, сети и телекоммуникации: Учебник. - 2-е изд., перераб. и доп. / Под ред. А.П. Пятибратова. - М.: Финансы и статистика, 2003.

13. Галатенко В.А. Стандарты информационной безопасности. - М.: Изд-во "Интернет-университет информационных технологий - ИНТУИТ.ру", 2004. - 328 с.: ил.
14. Гошко С.В. Энциклопедия по защите от вирусов. - М.: Изд-во "СОЛОН-Пресс", 2004. - 301 с.
15. Денисов А., Белов А., Вихарев И. Интернет. Самоучитель. - СПб.: Питер, 2000. - 464 с.: ил.
16. Журнал «Компьютерра» №2 (766) январь 2009г.
17. Зима В., Молдовян А., Молдовян Н. Безопасность глобальных сетевых технологий. Серия "Мастер". - СПб.: БХВ-Петербург, 2001. - 320 с.: ил.
18. Зубов А.Ю. Совершенные шифры. - М.: Гелиос АРВ, 2003. - 160 с., ил.
19. Касперски К. Записки исследователя компьютерных вирусов. - СПб.: Питер, 2004. - 320 с.: ил.
20. Козлов Д.А. Энциклопедия компьютерных вирусов. - М.: Изд-во "СОЛОН-Пресс", 2001. - 457 с.
21. Коул Э. Руководство по защите от хакеров. - М.: Издательский дом "Вильямс", 2002. - 640 с.
22. Лапонина О.Р. Криптографические основы безопасности. - М.: Изд-во "Интернет-университет информационных технологий - ИНТУИТ.ру", 2004. - 320 с.: ил.
23. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. - М.: Изд-во "Интернет-университет информационных технологий - ИНТУИТ.ру", 2005. - 608 с.: ил.
24. Мак-Клар С., Скембрей Дж., Курц Дж. Секреты хакеров. Безопасность сетей - готовые решения. 2-е издание. - М.: Издательский дом "Вильямс", 2001. - 656 с.
25. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. - СПб.: Питер, 2001. - 848 с.: ил.
26. Медведовский И.Д. Атака из Internet. - М.: Изд-во "СОЛОН-Пресс", 2002. - 368 с.

27. Микляев А.П., Настольная книга пользователя IBM PC 3-издание М.:, "Солон-Р", 2000, 720 с.
28. Норткат С., Новак Дж. Обнаружение нарушений безопасности в сетях. 3-е изд. - М.: Издательский дом "Вильямс", 2003. - 448 с.
29. Оглрти Т. Firewalls. Практическое применение межсетевых экранов – М.: ДМК, 2003. – 401 с.
30. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. - СПб.: Питер, 2002. - 864 с.: ил.
31. Партыка Т.Л., Попов И.И. Информационная безопасность. - М.:"Инфра-М", 2002. - 368 с.
32. Пархоменко П. Н., Яковлев С. А., Пархоменко Н. Г. Правовые аспекты проблем обеспечения информационной безопасности.– В сб. Материалы V Международной научно-практической конференции «Информационная безопасность».– Таганрог: ТРТУ, 2003.
33. Персональный компьютер: диалог и программные средства. Учебное пособие. Под ред. В.М. Матюшка - М.: Изд-во УДН, 2001.
34. Пятибратов А. П. Вычислительные системы, сети и телекоммуникации:Учебник; Под ред. А. П. Пятибратова. - 2-е изд., перераб. и доп. - М.:Финансы и статистика,2003. - 512 с.:ил. - Библиогр.: с. 495.
35. Расторгуев С. П. Философия информационной войны.– М.: Вузовская книга, 2001.– 468 с.
36. Симонис Д. и др. Check Point NG. Руководство по администрированию. - М.: ДМК Пресс, 2004. - 544 с.
37. Симонович С.В., Евсеев Г.А., Мураховский В.И. Вы купили компьютер: Полное руководство для начинающих в вопросах и ответах. - М.: АСТ-ПРЕСС КНИГА; Инфорком-Пресс, 2001,- 544 с.: ил.
38. Столлингс В. Криптография и защита сетей: принципы и практика. 2-е издание. - М.: Издательский дом "Вильямс", 2001. - 672 с.
39. Цвики Э., Купер С., Чапмен Б. Создание защиты в Интернете (2 издание). - СПб.: Символ-Плюс, 2002. - 928 с.

40. Ярочкин В.И. Информационная безопасность. - М.: Изд-во "Академический проект", 2004. - 640 с.

Список сокращений

СЭБ - Служба экономической безопасности

АИБ - Администратор информационной безопасности

АИС - Автоматизированная информационная система

АРМ - Автоматизированное рабочее место

АСУ - Автоматизированная система управления

ГТ - Государственная тайна

ДСП - Для служебного пользования

ЗИ - Защита информации

ИБ - Информационная безопасность

ИР - Информационный ресурс

ИТ - Информационные технологии

КТ - Коммерческая тайна

ЛВС - Локальная вычислительная сеть

МЭ - Межсетевой экран

НСД - Несанкционированный доступ

ОИ - Объект информатизации

ОС - Операционная система

ПЭВМ - Персональная электронная вычислительная машина

ПО - Программное обеспечение

ПТС - Программно-технические средства

СБП - Служба безопасности предприятия

СВТ - Средства вычислительной техники

СЗИ - Система защиты информации

СКЗИ - Средства криптозащиты информации

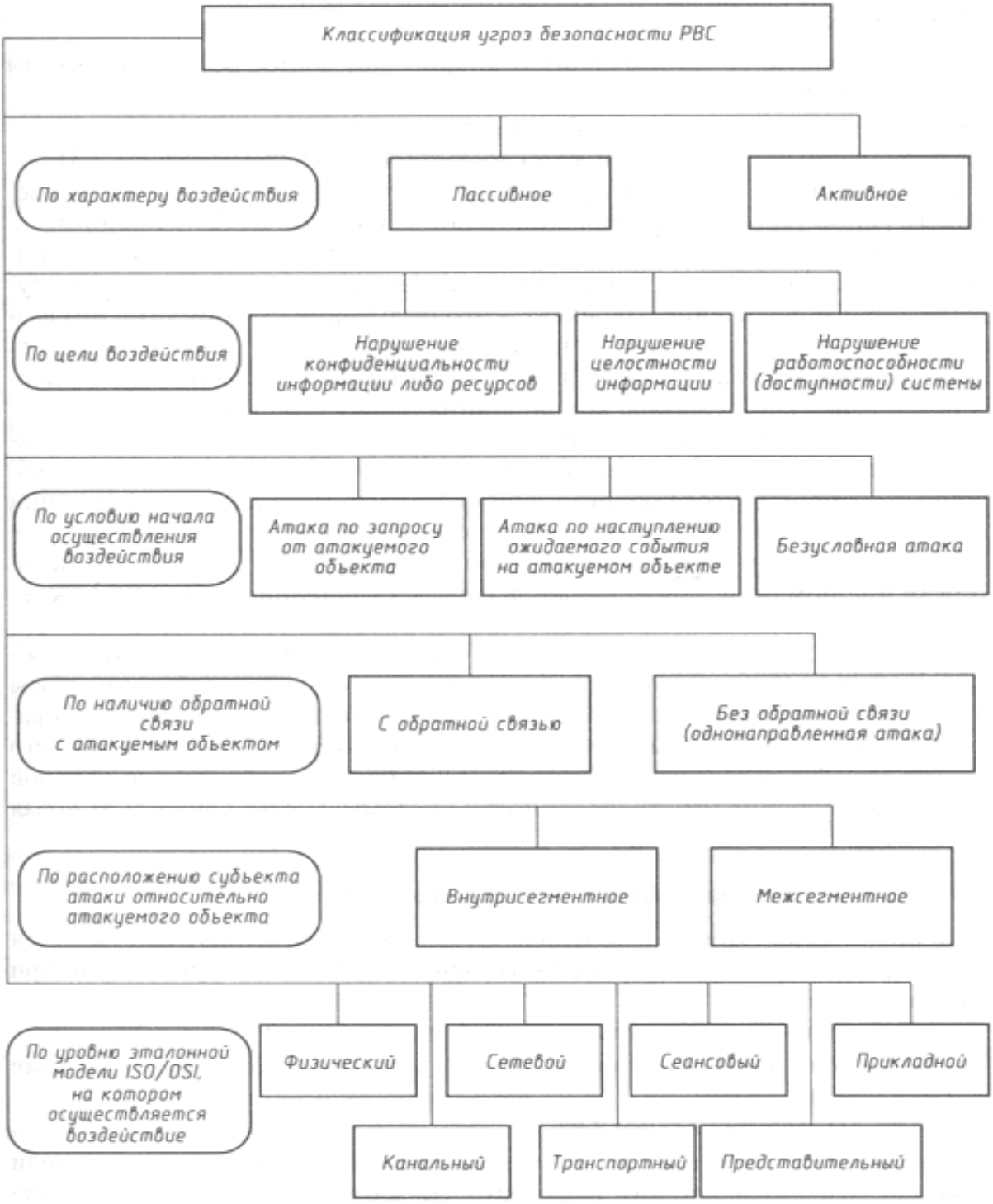
СОИ - Система обработки информации

ТСОИ - Техническое средство обработки информации

ЭЦП - Электронная цифровая подпись

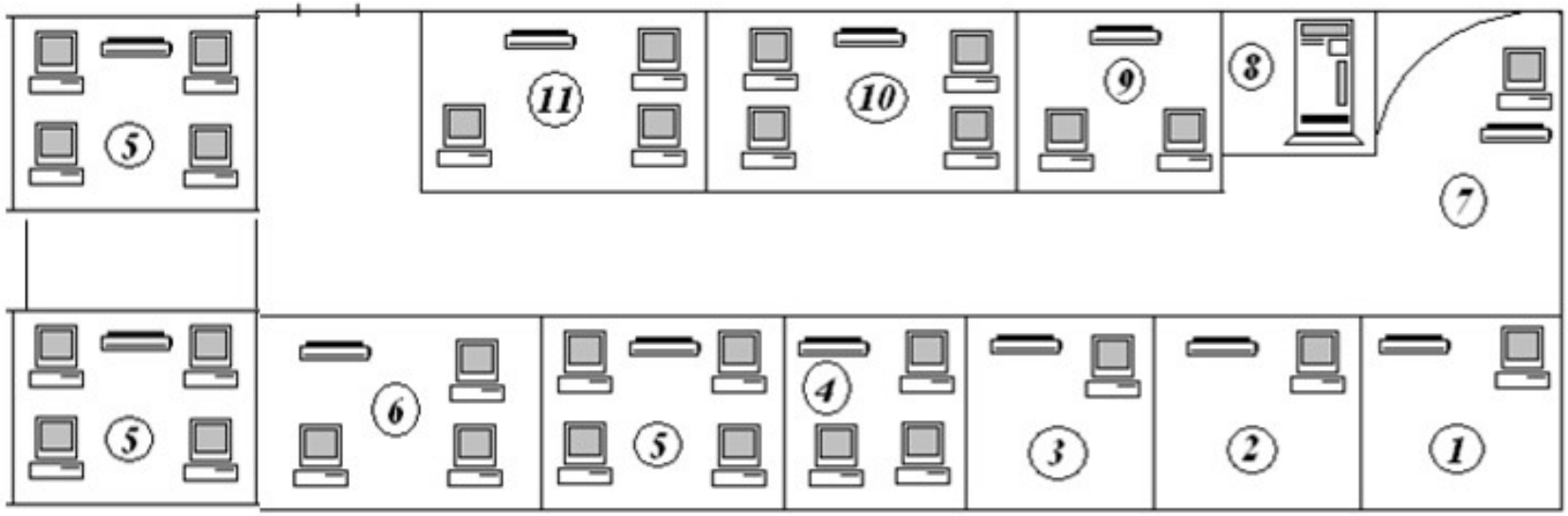
Приложение А

Классификация угроз безопасности



Приложение Б

План помещения



1. Кабинет директора предприятия.
2, 3. Отдел прямого подчинения.
4. Отделение 6 4-го отдеола.
5, 6. Отделения 4 и 5 3-го отдела.
7. Секретари.
8. Комната системного администратора.
9, 10, 11. Отделения 1, 2 и 3 1-го отдела.
12 Отдел 5
13 Отдел 6

Приложение В

Содержимое учетной карточки.

Учетная карточка пользователя.	Элемент учетной карточки.	Комментарии.
Username	Имя пользователя	Уникальное имя пользователя, выбирается при регистрации.
Password	Пароль	Пароль пользователя.
Full name	Полное имя	Полное имя пользователя.
Logon hours	Часы начала сеанса	Часы, в течение которых пользователю позволяется входить в систему. Они влияют на вход в систему сети и доступ к серверу. Так или иначе, пользователь вынужден будет выйти из системы, когда его часы сеанса, определенные политикой безопасности, истекут.
Logon workstations	Рабочие станции	Имена рабочих станций, на которых пользователю позволяется работать. По умолчанию пользователь может использовать любую рабочую станцию, но возможно введение ограничений.
Expiration date	Дата	Дата в будущем, когда учетную карточку автоматически исключают из базы, полезна при принятии на работу временных служащих
Home directory	Собственный каталог	Каталог на сервере, который принадлежит пользователю; пользователь управляет доступом к этому каталогу.
Logon script	Сценарий начала сеанса	Пакетный или исполняемый файл, который запускается автоматически, когда пользователя начинает сеанс.
Profile	Установки (параметры)	Файл, содержащий запись о параметрах среды рабочего стола (Desktop) пользователя, о таких, например, как сетевые соединения, цвета экрана и установочные параметры, определяющие, какие аспекты среды, пользователь может изменить.
Account type	Тип учетной карточки	Тип учетной карточки - глобальный или локальный.

Приложение Г

Вероятностная методика оценки качества антивируса

Методика оценки качества антивирусов основана на вычислении вероятности антивируса противостоять атакам вредоносных объектам, которые реально угрожали компьютерной системе. Численное значение такой оценки можно рассчитать по формуле:

$$Pav = (Nvir - Nbad) / Nvir$$

Где:

Pav - Вероятностная оценка качества антивируса, чем она ближе к единице, тем лучше антивирус.

Nvir- Общее число зафиксированных вредоносных объектов на данном компьютере (организации).

Nbad - Число вредоносных объектов, которые антивирус в момент атаки не выявил.

Таблица 1 содержит расчеты показателя надежности (последняя колонка) различных антивирусов. В качестве исходных данных были использованы результаты проверки реакции различных антивирусов на реальные вредоносные объекты.

Общее число зафиксированных вредоносных объектов было 51. Расчетные показатели надежности различных антивирусов приведены в таблице 1.

Таблица 1. Показатели надежности антивирусов

Наименование антивируса	Пропущено вирусов за соответствующий период 2006 - 2007 годов												Пропущено вирусов из 51 атак	Качество антивируса
	10.12 -	17.05	05.06 -	12.07	17.07	21.07	24-26.07	27.07	27.07	30.07	31.07	03.08		
DrWeb	12	1	0	0	0	0	3	0	0	1	0	0	17	0,667
Kaspersky	11	1	3	1	0	0	2	1	0	0	1	1	21	0,588
AntiVir	13	1	2	0	2	1	0	0	1	0	1	1	22	0,569
Fortinet	14	1	0	0	2	2	1	0	1	1	1	1	23	0,549
Sophos	19	1	0	0	0	1	0	0	1	1	1	0	24	0,529
BitDefender	14	1	3	0	2	1	0	1	1	1	1	1	25	0,510
McAfee	19	0	1	0	2	2	0	0	1	1	0	1	27	0,471
Ikarus	19	1	1	0	2	1	1	0	1	0	1	0	27	
eSafe	15	1	4	1	1	2	3	1	1	0	0	0	28	0,451
NOD32v2	16	1	4	0	2	1	0	1	1	1	1	1	29	0,431
CAT-QuickHeal	19	0	3	0	2	2	0	1	1	0	1	1	30	0,412
ClamAV	16	0	3	1	2	2	2	1	1	1	1	1	31	0,392
VBA32	18	0	4	0	1	1	2	1	1	1	1	1	31	
Sunbelt	20	1	3	0	2	2	0	1	1	0	1	1	32	0,373
Norman	21	1	1	1	1	1	3	0	1	1	1	0	32	
F-Prot	16	1	4	1	2	2	3	1	1	1	1	1	33	0,353
Microsoft	26	1	1	0	0	1	0	0	1	1	1	1	33	
Panda	19	1	4	0	2	2	1	1	1	0	1	1	33	
Authentium	16	1	4	1	2	2	3	1	1	1	1	1	34	0,333
AVG	18	1	4	0	2	2	2	1	1	1	1	1	34	
TheHacker	23	1	2	1	1	1	3	0	1	1	1	1	36	0,294

Ewido	22	1	4	1	2	1	3	1	1	1	1	1	38	0,255
Avast	25	0	4	1	2	2	0	1	1	1	1	0	39	0,235