УЗБЕКСКОЕ АГЕНТСТВО СВЯЗИ И ИНФОРМАТИЗАЦИИ
ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра “Информационная безопасность”

На правах рукописи

Миносян Сергей Радиевич

Организация комплексной системы мониторинга безопасности компьютерных сетей

Специальность: 5А523509

ДИССЕРТАЦИЯ
на соискание академической степени магистра
по специальности “Информационная безопасность”

Работа рассмотрена и
допускается к защите
Зав. Кафедрой ИБ
к.т.н., доцент Юсупов С.С.

_____
“___”_____2012 г.

Научный руководитель
д.т.н., академик
Бекмуратов Т.Ф.

_____
“___” _____2012

Ташкент – 2012

ОГЛАВЛЕНИЕ

Введение

В Республике Узбекистан ускоренными темпами развивается национальная инфраструктура информационных технологий. На открытии международной конференции «Подготовка образованного и интеллектуально развитого поколения – как важнейшее условие устойчивого развития и модернизации страны» 2012 году Президента Республики Узбекистан Ислама Каримов отметил: «Важное место в реформировании образовательного процесса и подготовке высококвалифицированных кадров, востребованных на рынке труда, занимают высшие учебные заведения. В стенах этих вузов готовят бакалавров и магистров по таким востребованным на рынке труда специальностям, как машиностроение, нефтегазовое дело, информационные технологии, экономика и управление бизнесом, финансовый менеджмент, коммерческое право, и их выпускники получают, что очень важно для нас, дипломы, признаваемые во всем мире.» Это свидетельствует о том, что за годы независимости республики произошли кардинальные изменения в жизни общества, изменились цели и задачи, состоящие сегодня перед экономикой, телекоммуникационной отраслью, информационной индустрию.

Актуальность темы диссертационной работы. Задача анализа защищенности компьютерных сетей на различных этапах их жизненного цикла, основными из которых являются этапы проектирования и эксплуатации, все чаще становится объектом обсуждения на специализированных конференциях, посвященных обеспечению информационной безопасности [10]. Такое пристальное внимание к данной задаче объясняется тем, что анализ защищенности необходим при контроле и мониторинге защищенности компьютерных сетей, при аттестации автоматизированных систем (компьютерных сетей) и сертификации средств вычислительной техники по требованиям действующих нормативных документов и требует обработки большого объема данных в условиях дефицита времени. Мониторинг корпоративной сети в целях обеспечения информационной безопасности.

Под мониторингом корпоративной сети обычно понимается технология наблюдения за ресурсами сети, генерации сигналов тревоги и выработки адекватных диагностических решений. Организация процедур мониторинга является одним из необходимых условий реализации комплексной политики безопасности. Решение комплексной проблемы организации мониторинга корпоративной сети подразделяется на выполнение ниже перечисленных взаимосвязанных задач:

- декодирование и анализ сетевых пакетов;
- мониторинг активного сетевого оборудования;
- мониторинг состояния кабельной системы;
- мониторинг состояния серверов и ответственных рабочих станций;
- мониторинг приложений.

При анализе защищенности компьютерных сетей во внимание следует принимать все разновидности угроз, однако наибольшее внимание должно быть уделено тем из них, которые связаны с действиями человека, злонамеренными или иными [18]. Поэтому как естественные угрозы, в данной работе рассматриваются угрозы искусственного характера.

Степень изученности проблемы. Исследование теоретических и практических аспектов проблем обеспечения информационной безопасности, различных подходам к их решению, методам построение защищенных компьютерных сетей и систем посвящены многочисленные работы ученых, таких как В.А.Герасименко, Д.П.Зегжда, Harrison M., Р.М.Алгулиева, С.К.Ганиева и многих других. Однако, к настоящему времени вопросы выбора и применения конкретных моделей мониторинга безопасности к компьютерным сетям недостаточно проработаны.

Цель работы и задачи исследования. Основной целью диссертационной работы является повышение эффективности анализа защищенности компьютерных сетей на этапах проектирования и эксплуатации на основе разработки и использования моделей компьютерных атак, нарушителя,

анализируемой компьютерной сети, оценки уровня защищенности и методики анализа защищенности компьютерных сетей.

Для достижения данной цели в диссертационной работе поставлены и решены следующие **задачи**:

1) Анализ существующих методов и средств анализа защищенности КС на этапах проектирования и эксплуатации для выделения их достоинств и недостатков, определения требований к ним;

2) Анализ современных методов и средств мониторинга систем безопасности;

3) Разработка алгоритма функционирования системы мониторинга безопасности корпоративных сетей;

4) Разработка программного средства для автоматизации анализа защищенности компьютерных сетей на этапах проектирования и эксплуатации, позволяющего оценить эффективность предложенной методики.

Объект и предмет исследования. Объектом исследования является информационная безопасность компьютерных сетей. Предметом исследования являются структурные методы мониторинга, модель мониторинга безопасности компьютерных сетей, алгоритм и программные средства защиты информации.

Основные положение выносимые на защиту:

- методы и средства анализа защищенности КС на этапах проектирования и эксплуатации для выделения их достоинств и недостатков, определения требований к ним;
- современных методы и средства мониторинга систем безопасности;
- алгоритм функционирования системы мониторинга безопасности корпоративных сетей;

Научная новизна работы заключается в следующем:

- Предложен метод мониторинга безопасности при функционировании инфокоммуникационной системы, что позволяет при анализе параметров

мониторинга учитывать характеристики загрузки вычислительных ресурсов, параметров уязвимостей и защищенности.

- Разработаны алгоритм и программный модуль мониторинга безопасности на примере использования Internet-ресурсов, позволяющий получить статистические данные о сетевом трафике.

Научная и практическая значимость результатов исследования.

Научная значимость результатов диссертационной работы заключает в разработке метода мониторинга безопасности компьютерных сетей примере использования Internet-ресурсов, позволяющий получить статистические данные о сетевом трафике для повышение уровня защищенности.

Практическая значимость результатов исследования диссертационной работы заключается в том, что предложенные метод мониторинга выявляет уязвимые точки и повысить защищенность от несанкционированных воздействие и надежное функционирование компьютерных сетей.

Структура и объем диссертационной работы. Диссертационная работа объемом 109 машинописные страницы, содержит введение, три главы и заключение, список литературы, содержащий 17 наименований, 9 таблиц, 34 рисунков и листинг программы. В приложениях приведен пример использования разработанного программного прототипа системы анализа защищенности.

ГЛАВА 1. ПРОБЛЕМЫ ОРГАНИЗАЦИИ КОМПЛЕКСНОЙ СИСТЕМЫ МОНИТОРИНГА БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ.

1.1. Основные цели обеспечения информационной безопасности в компьютерных сетях

Цели обеспечения информационной безопасности в компьютерных сетях могут меняться в зависимости от ситуации, но основными считаются следующие:

- целостность данных;
- конфиденциальность данных;
- доступность данных.

Рассмотрим более подробно каждую из них.

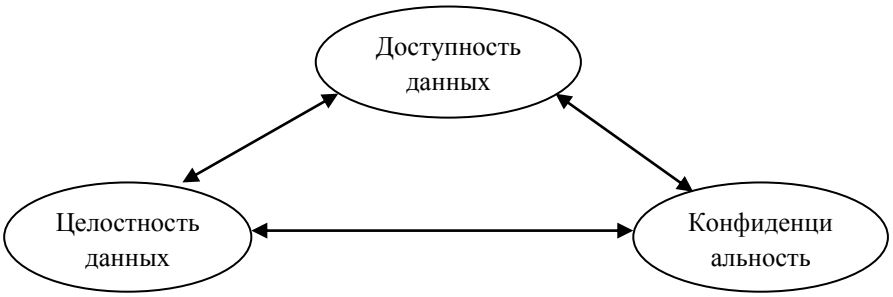


Рис. 1.1. Основные цели сетевой безопасности.

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

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

открытых, является основной задачей. К конфиденциальной информации можно отнести следующие данные:

- Личная информация пользователей.
- Учетные записи (имена и пароли).
- Данные о кредитных картах.
- Данные о разработках и различные внутренние документы.
- Бухгалтерская информация.

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

- Принтеры.
- Серверы.
- Рабочие станции.
- Данные пользователей.
- Любые критические данные, необходимые для работы.

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

Технические угрозы:

- Ошибки в программном обеспечении.
- Различные DoS- и DDoS-атаки.
- Компьютерные вирусы, черви, троянские кони.
- Анализаторы протоколов и прослушивающие программы ("снифферы").
- Технические средства съема информации.

Ошибки в программном обеспечении. Самое узкое место любой сети. Программное обеспечение серверов, рабочих станций, маршрутизаторов и т. д. написано людьми, следовательно, оно практически всегда содержит ошибки.

Чем выше сложность подобного ПО, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляет никакой опасности, некоторые же могут привести к трагическим последствиям, таким, как получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов (хранение ненужных данных на сервере, использование в качестве плацдарма для атаки и т.п.). Большинство таких уязвимостей устраняется с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких обновлений является необходимым условием безопасности сети.

DoS- и DDoS-атаки. Denial Of Service (отказ в обслуживании) - особый тип атак, направленный на выведение сети или сервера из работоспособного состояния. При DoS-атаках могут использоваться ошибки в программном обеспечении или легитимные операции, но в больших масштабах (например, посылка огромного количества электронной почты). Новый тип атак DDoS (Distributed Denial Of Service) отличается от предыдущего наличием огромного количества компьютеров, расположенных в большой географической зоне. Такие атаки просто перегружают канал трафиком и мешают прохождению, а зачастую и полностью блокируют передачу по нему полезной информации. Особенно актуально это для компаний, занимающихся каким-либо online-бизнесом, например, торговлей через Internet.

Компьютерные вирусы, троянские кони. Вирусы - старая категория опасностей, которая в последнее время в чистом виде практически не встречается. В связи с активным применением сетевых технологий для передачи данных вирусы все более тесно интегрируются с троянскими компонентами и сетевыми червями. В настоящее время компьютерный вирус использует для своего распространения либо электронную почту, либо уязвимости в ПО. А часто и то, и другое. Теперь на первое место вместо деструктивных функций вышли функции удаленного управления, похищения информации и использования зараженной системы в качестве плацдарма для дальнейшего распространения. Все чаще зараженная машина становится

активным участником DDoS-атак. Методов борьбы достаточно много, одним из них является все та же своевременная установка обновлений.

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

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

Человеческий фактор:

- Уволенные или недовольные сотрудники.
- Промышленный шпионаж.
- Халатность.
- Низкая квалификация.

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

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

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

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

1.2. Методы защиты компьютерных сетей

Согласно статистике потерь, которые несут организации от различных компьютерных преступлений, львиную долю занимают потери от преступлений, совершаемых собственными нечистоплотными сотрудниками. Однако в последнее время наблюдается явная тенденция к увеличению потерь от внешних злоумышленников. В любом случае необходимо обеспечить защиту

как от нелояльного персонала, так и от способных проникнуть в вашу сеть хакеров. Только комплексный подход к защите информации может внушить уверенность в ее безопасности.

Однако в связи с ограниченным объемом данной статьи рассмотрим только основные из технических методов защиты сетей и циркулирующей по ним информации, а именно - криптографические алгоритмы и их применение в данной сфере.

Защита данных от внутренних угроз. Для защиты циркулирующей в локальной сети информации можно применить следующие криптографические методы:

шифрование информации;

электронную цифровую подпись (ЭЦП).

Шифрование. Шифрование информации помогает защитить ее конфиденциальность, т.е. обеспечивает невозможность несанкционированного ознакомления с ней. Шифрование - это процесс преобразования открытой информации в закрытую, зашифрованную (что называется "зашифрование") и наоборот ("расшифрование"). Это преобразование выполняется по строгим математическим алгоритмам; помимо собственно данных в преобразовании также участвует дополнительный элемент - "ключ". Иными словами, ключ представляет собой уникальный элемент, позволяющий зашифровать информацию так, что получить открытую информацию из зашифрованной можно только определенному пользователю или группе пользователей.

Шифрование можно выразить следующими формулами:

C=Ek1 (M) - зашифрование,

M"=Dk2(C) - расшифрование.

Функция E выполняет зашифрование информации, функция D – расшифрование. В том случае, если ключ k2 соответствует ключу k1, примененному при зашифровании, удается получить открытую информацию, т.е. получить соответствие M" = M.

При отсутствии же правильного ключа k2 получить исходное сообщение практически невозможно.

По виду соответствия ключей k1 и k2 алгоритмы шифрования разделяются на две категории:

1) Симметричное шифрование: k1 = k2. Для зашифрования и расшифрования информации используется один и тот же ключ. Это означает, что пользователи, обменивающиеся зашифрованной информацией, должны иметь один и тот же ключ. Более безопасный вариант - существует уникальный ключ шифрования для каждой пары пользователей, который неизвестен остальным. Ключ симметричного шифрования должен храниться в секрете: его компрометация (утеря или хищение) повлечет за собой раскрытие всей зашифрованной данным ключом информации.

2) Асимметричное шифрование. Ключ k1- в данном случае называется "открытым", а ключ k2 - "секретным". Открытый ключ вычисляется из секретного различными способами (зависит от конкретного алгоритма шифрования). Обратное же вычисление k2 из k1 является практически невозможным. Смысл асимметричного шифрования состоит в том, что ключ k2 хранится в секрете у его владельца и не должен быть известен никому; ключ k1, наоборот, распространяется всем пользователям, желающим отправлять зашифрованные сообщения владельцу ключа k2; любой из них может зашифровать информацию на ключе k1, расшифровать же ее может только обладатель секретного ключа k2.

Оба ключа: ключ симметричного и секретный ключ асимметричного шифрования должны быть абсолютно случайными - в противном случае злоумышленник теоретически имеет возможность спрогнозировать значение определенного ключа. Поэтому для генерации ключей обычно используют датчики случайных чисел (ДСЧ), лучше всего - аппаратные.

Электронная цифровая подпись (ЭЦП). ЭЦП позволяет гарантировать целостность и авторство информации (Рис.1.2). Как видно из схемы, ЭЦП также использует криптографические ключи: секретный и открытый. Открытый

ключ вычисляется из секретного по достаточно легкой формуле, например: y=ax mod p (где x - секретный ключ, y - открытый ключ, a и p- параметры алгоритма ЭЦП), обратное же вычисление весьма трудоемко и считается неосуществимым за приемлемое время при современных вычислительных мощностях.

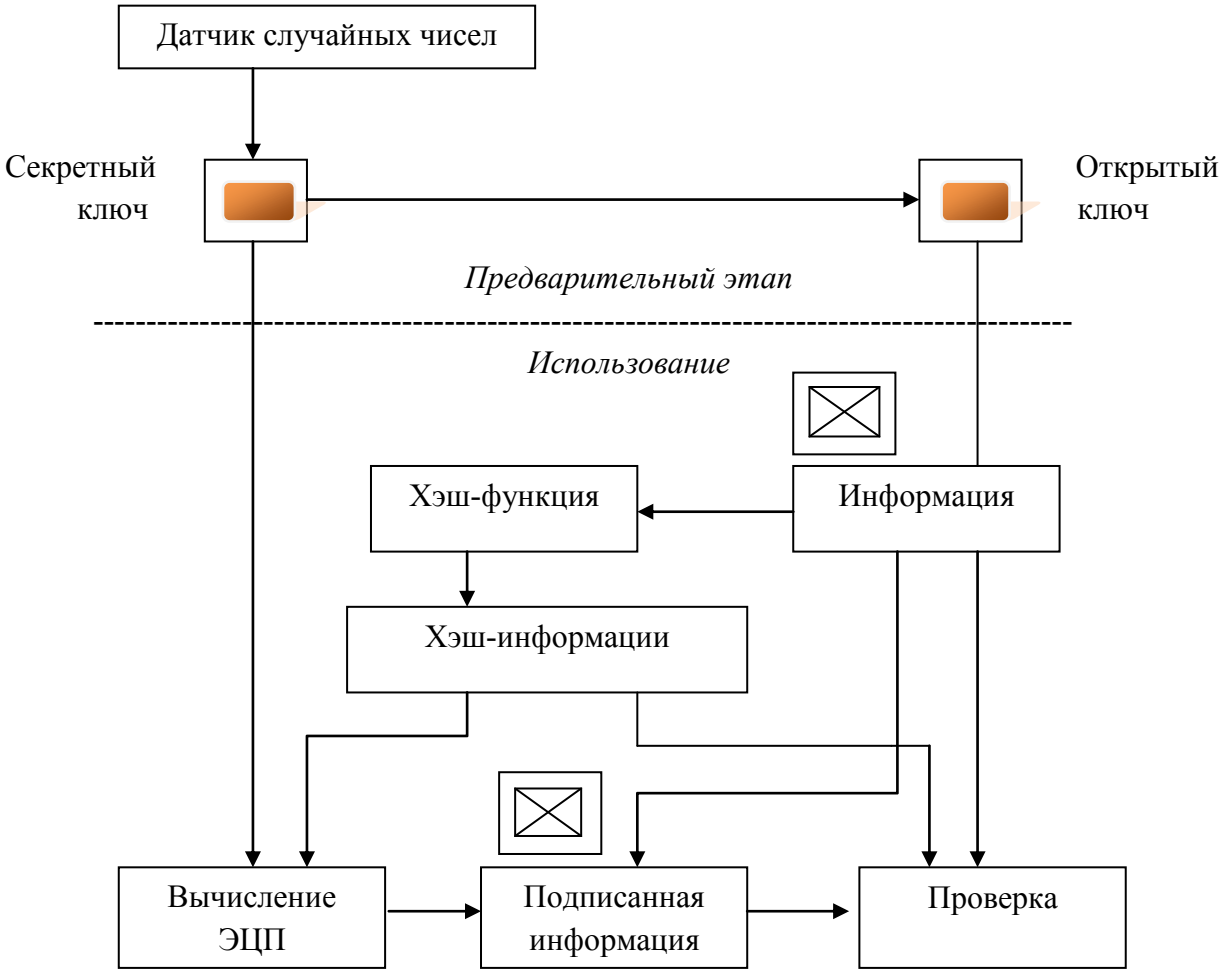


Рис.1.2. Схема применения ЭЦП

Схема распространения ключей ЭЦП аналогична схеме асимметричного шифрования: секретный ключ должен оставаться у его владельца, открытый же распространяется всем пользователям, желающим проверять ЭЦП владельца секретного ключа. Необходимо обеспечивать недоступность своего секретного ключа, ибо злоумышленник легко может подделать ЭЦП любого пользователя, получив доступ к его секретному ключу.

Электронной подписью можно подписать любую информацию. Предварительно информацию обрабатывают функцией хэширования, цель

которой - выработка последовательности определенной длины, однозначно отражающей содержимое подписываемой информации. Данная последовательность называется "хэш", основное свойство хэша таково, что исключительно сложно модифицировать информацию так, чтобы ее хэш остался неизменным.

На основе хэша информации и секретного ключа пользователя вычисляется ЭЦП. Как правило, ЭЦП отправляется вместе с подписанной информацией (ЭЦП файла чаще всего просто помещают в конец файла перед его отправкой куда-либо по сети). Сама ЭЦП, как и хэш, является бинарной последовательностью фиксированного размера. Однако, помимо ЭЦП, к информации обычно добавляется также ряд служебных полей, прежде всего, идентификационная информация о пользователе, поставившем ЭЦП; причем, данные поля участвуют в расчете хэша.

Естественно, в случае неверной ЭЦП выводится соответствующая информация, содержащая причину признания ЭЦП неверной. При проверке ЭЦП также вычисляется хэш информации; если он не совпадает с полученным при вычислении ЭЦП (что может означать попытку модификации информации злоумышленником), ЭЦП будет неверна.

Существует и более простой способ обеспечения целостности информации - вычисление имитоприставки. Имитоприставка - это криптографическая контрольная сумма информации, вычисляемая с использованием ключа шифрования. Для вычисления имитоприставки используется, в частности, один из режимов работы алгоритма ГОСТ 28147-89, позволяющий получить в качестве имитоприставки 32-битную последовательность из информации любого размера. Аналогично хэшу информации имитоприставку чрезвычайно сложно подделать. Использование имитоприставок более удобно, чем применение ЭЦП: во-первых, 4 байта информации намного проще добавить, например, к пересылаемому по сети IP-пакету, чем большую структуру ЭЦП, во-вторых, вычисление имитоприставки существенно менее ресурсоемкая операция, чем формирование ЭЦП, поскольку в последнем случае

используются такие сложные операции, как возведение 512-битного числа в степень, показателем которой является 256-битное число, что требует достаточно много вычислений. Имитоприставку нельзя использовать для контроля авторства сообщения, но этого во многих случаях и не требуется.

Комплексное применение криптографических алгоритмов. Для безопасной передачи по сети каких-либо файлов, их достаточно подписать и зашифровать. На Рис.1.3 представлена технология специализированного архивирования, обеспечивающая комплексную защиту файлов перед отправкой по сети.

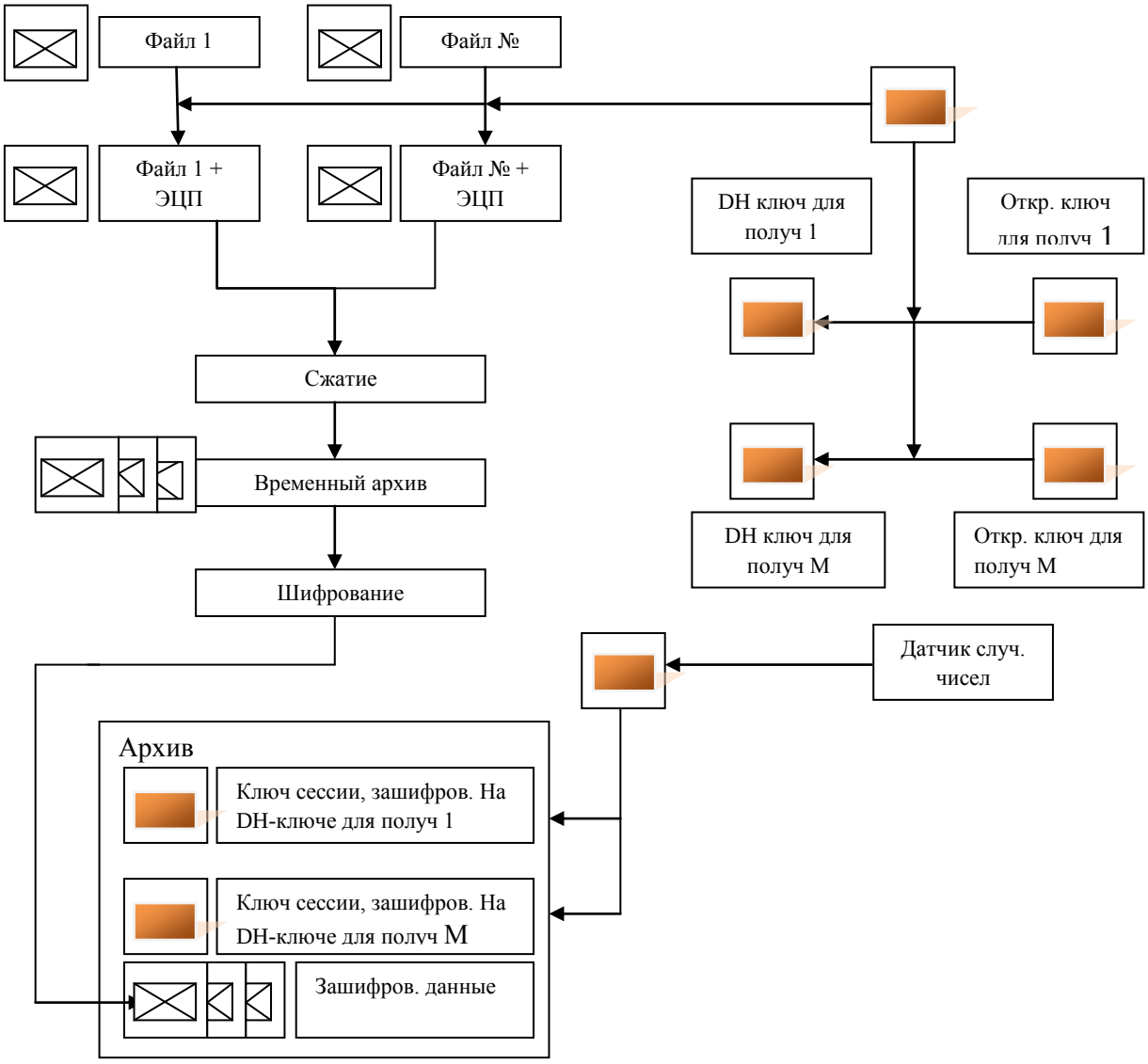


Рис.1.3. Технология специализированного архивирования

Прежде всего, файлы подписываются секретным ключом отправителя, затем сжимаются для более быстрой передачи. Подписанные и сжатые файлы

шифруются на случайном ключе сессии, который нужен только для зашифрования этой порции файлов -ключ берется с датчика случайных чисел, который обязан присутствовать в любом шифраторе. После этого к сформированному таким образом спецархиву добавляется заголовок, содержащий служебную информацию.

Заголовок позволяет расшифровать данные при получении. Для этого он содержит ключ сессии в зашифрованном виде. После зашифрования данных и записи их в архив, ключ сессии, в свою очередь, зашифровывается на ключе парной связи (DH-ключ), который вычисляется динамически из секретного ключа отправителя файлов и открытого ключа получателя по алгоритму Диффи-Хеллмана. Ключи парной связи различны для каждой пары "отправитель-получатель". Тот же самый ключ парной связи может быть вычислен только тем получателем, открытый ключ которого участвовал в вычислении ключа парной связи на стороне отправителя. Получатель для вычисления ключа парной связи использует свой секретный ключ и открытый ключ отправителя. Алгоритм Диффи-Хеллмана позволяет при этом получить тот же ключ, который сформировал отправитель из своего секретного ключа и открытого ключа получателя.

Таким образом, заголовок содержит копии ключа сессии (по количеству получателей), каждая их которых зашифрована на ключе парной связи отправителя для определенного получателя.

После получения архива получатель вычисляет ключ парной связи, затем расшифровывает ключ сессии, и наконец, расшифровывает собственно архив. После расшифрования информация автоматически разжимается. В последнюю очередь проверяется ЭЦП каждого файла.

Защита от внешних угроз. Методов защиты от внешних угроз придумано немало - найдено противодействие практически против всех опасностей, перечисленных в первой части данной статьи. Единственная проблема, которой пока не найдено адекватного решения, - DDoS-атаки. Рассмотрим технологию виртуальных частных сетей (VPN - Virtual Private Network), позволяющую с

помощью криптографических методов как защитить информацию, передаваемую через Internet, так и пресечь несанкционированный доступ в локальную сеть снаружи.

Виртуальные частные сети. На наш взгляд, технология VPN является весьма эффективной защитой, ее повсеместное внедрение - только вопрос времени. Доказательством этого является хотя бы внедрение поддержки VPN в последние операционные системы фирмы Microsoft - начиная с Windows 2000.

Суть VPN состоит в следующем (см. Рис.1.4.):

На все компьютеры, имеющие выход в Internet (вместо Internet может быть и любая другая сеть общего пользования), ставится средство, реализующее VPN. Такое средство обычно называют VPN-агентом. VPN-агенты обязательно должны быть установлены на все выходы в глобальную сеть.

VPN-агенты автоматически зашифровывают всю информацию, передаваемую через них в Internet, а также контролируют целостность информации с помощью имитоприставок.

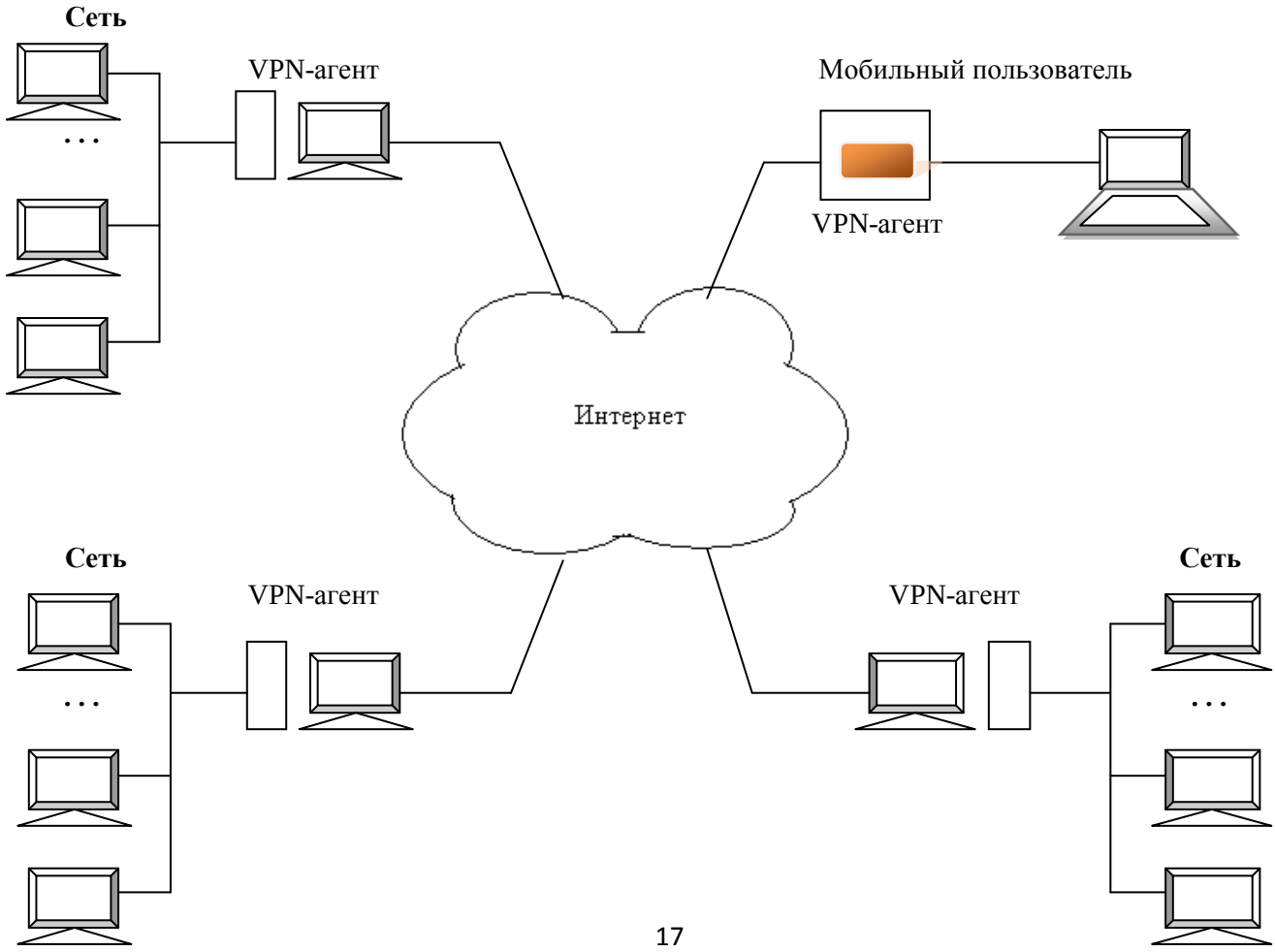


Рис. 1.4 Технология VPN

Как известно, передаваемая в Internet информация представляет собой множество пакетов протокола IP, на которые она разбивается перед отправкой и может многократно переразбиваться по дороге. VPN-агенты обрабатывают именно IP-пакеты, ниже описана технология их работы.

1. Перед отправкой IP-пакета VPN-агент выполняет следующее:

Анализируется IP-адрес получателя пакета. В зависимости от адреса и другой информации (см. ниже) выбираются алгоритмы защиты данного пакета (VPN-агенты могут, поддерживать одновременно несколько алгоритмов шифрования и контроля целостности) и криптографические ключи. Пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится. Вычисляется и добавляется в пакет его имитоприставка.

Пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию).

Формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента. Это называется инкапсуляцией пакета. При использовании инкапсуляции обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например, внутренние IP-адреса сети, в этом случае недоступна.

2. При получении IP-пакета выполняются обратные действия:

Из заголовка пакета получается информация о VPN-агенте отправителя пакета. Если такой отправитель не входит в число разрешенных в настройках, то пакет отбрасывается. То же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком.

Согласно настройкам выбираются криптографические алгоритмы и ключи.

Пакет расшифровывается, затем проверяется его целостность. Пакеты с нарушенной целостностью также отбрасываются.

В завершение обработки пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложной является только настройка VPN-агентов, которая может быть выполнена только очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера - на котором установлен.

VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (к таким каналам обычно применяется термин "туннель", а технология их создания называется "туннелировани-ем"). Вся информация идет по туннелю только в зашифрованном виде. Кстати, пользователи VPN при обращении к компьютерам из удаленных локальных сетей могут и не знать, что эти компьютеры реально находятся, может быть, в другом городе, - разница между удаленными и локальными компьютерами в данном случае состоит только в скорости передачи данных.

Как видно из описания действий VPN-агентов, часть IP-пакетов ими отбрасывается. Действительно, VPN-агенты фильтруют пакеты согласно своим настройкам (совокупность настроек VPN-агента называется "Политикой безопасности"). То есть VPN-агент выполняет два основных действия: создание туннелей и фильтрация пакетов (см.Рис. 1.5).

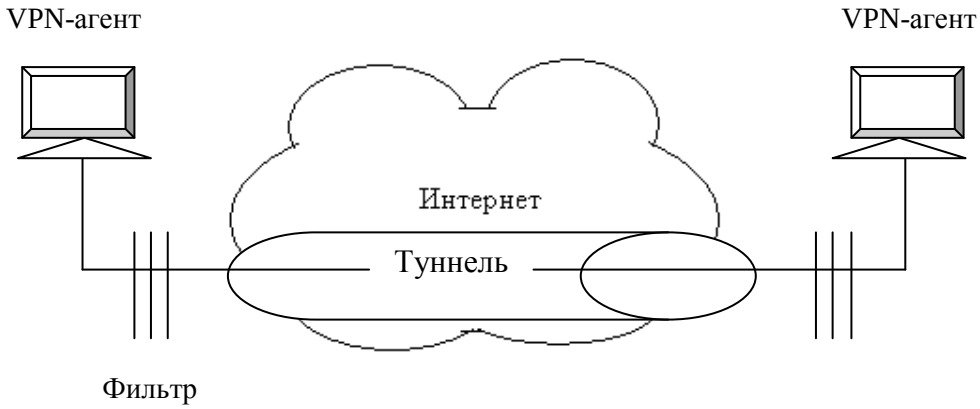


Рис. 1.5. Туннелирование и фильтрация

IP-пакет отбрасывается или направляется в конкретный туннель в зависимости от значений следующих его характеристик:

- IP-адрес источника (для исходящего пакета - адрес конкретного компьютера защищаемой сети).
- IP-адрес назначения.
- Протокол более верхнего уровня, которому принадлежит данный пакет (например, TCP или UDP для транспортного уровня).
- Номер порта, с которого или на который отправлен пакет (например, 1080).

1.3. Методы мониторинга и обеспечения безопасности для поддержания работоспособности корпоративной сети

В начале развития компьютерных сетей считалось, что эффективная защита может быть обеспечена применением традиционных услуг безопасности (паролированием и разграничением доступа, криптографией и т.д.) и, для сетей, имеющих выход в internet, использованием межсетевых экранов. Сегодня общепринятым является подход, включающий постоянный (24 часа в день, 7 дней в неделю) контроль за трафиком корпоративной сети на предмет обнаружения вторжений (мониторинг сети) и периодическое проведение анализа сети на наличие уязвимостей (аудит сети).

Задача контроля трафика решается при помощи так называемых систем обнаружения вторжения (intrusion detection systems, ids). ids, в зависимости от технологий защиты, которые они реализуют, бывают двух видов: ids сетевого уровня (сети) и ids системного уровня (хоста).

Для решения задачи анализа сети на наличие уязвимостей должен существовать инструмент, позволяющий выявлять и анализировать уязвимости сети и выдавать рекомендации по их устранению. такие инструменты есть и называются они средствами анализа защищенности (за рубежом эти средства

называют сканирующим обеспечением, или просто сканерами, а также сканерами безопасности).

Сегодня ведущие разработчики соответствующего программного обеспечения все чаще реализуют сетевой мониторинг и аудит в едином изделии («в одном флаконе»).

Мониторинг корпоративной сети в целях обеспечения информационной безопасности. Под мониторингом корпоративной сети обычно понимается технология наблюдения за ресурсами сети, генерации сигналов тревоги и выработки адекватных диагностических решений. организация процедур мониторинга является одним из необходимых условий реализации комплексной политики безопасности. решение комплексной проблемы организации мониторинга корпоративной сети подразделяется на выполнение ниже перечисленных взаимосвязанных задач:

- декодирование и анализ сетевых пакетов;
- мониторинг активного сетевого оборудования;
- мониторинг состояния кабельной системы;
- мониторинг состояния серверов и ответственных рабочих станций;
- мониторинг приложений.

Организация сетевого мониторинга является очень сложной задачей в случае гетерогенных сетей и существенно проще в случае однородных сетей.

Существуют два подхода к организации мониторинга :

установка комплексной системы (единое программно-аппратное решение; более дорогостоящий вариант);

организация мониторинга на основе множества продуктов.

В основе мониторинга безопасности лежит анализ сетевого трафика. в частном случае задача анализа трафика решается на основе применения сетевых анализаторов (анализаторов протоколов).

Анализаторы протоколов – программные или программно-аппаратные изделия для изучения особенностей трафика (вплоть до содержимого пакетов) в

конкретном сегменте сети. программно-аппаратные решения подразумевают использование специальных ноутбуков, снабженных различными коммутационными портами и датчиками. стоимость подобных изделий – десятки тысяч долларов. стоимость программных решений на порядок дешевле, но они требуют выделения сетевого компьютера под соответствующие цели.

Важнейшим элементом любого анализатора вторжений является декодирующее ядро (engine). этот модуль осуществляет декодирование захваченных пакетов с точностью до значений полей. особенности процесса декодирования определяются точностью настройки фильтра, стоящего на входе. в некоторых анализаторах реализована достаточно гибкая система фильтрации (создание фильтров отбирающих из трафика необходимые пакеты с точностью до поля) - анализатор lansleuth. в других анализаторах осуществляется фильтрация трафика с точностью до протокола (анализатор etherpeak). информация, вырабатываемая модулем engine является основным анализируемым информационным ресурсом. генератор сигналов тревоги как правило обладает средствами настройки на сигнатуры возможных атак и неисправностей. в различных моделях анализаторов протоколов этот модуль способен вырабатывать звуковой сигнал а также посылать сообщения на пейджер и факс, используя при этом возможности анализируемой сети. индикация в реальном масштабе времени основных показателей жизнеспособности сети является существенной компонентой некоторых типов анализаторов протоколов. это так называемая группа показателей - network vital signs. этот механизм неплохо реализован в анализаторах семейства linkviewpro.

Анализаторы протоколов снабжаются все более развитой системой фильтров и генераторами сигналов тревоги, позволяющими выдавать диагностические сообщения на сетевые устройства, пейджер или факс, некоторые системы обладают способностью формирования правил безопасности. но всех этих функций явно недостаточно для полномасштабной реализации политики безопасности.

Активное изучение применения анализаторов протоколов как средства предотвращения возможных атак на информационные ресурсы сети привело к появлению принципиально нового класса систем — систем мониторинга безопасности. любая такая система обязательно включает в свой состав декодирующий анализатор протоколов и библиотеку сигнатур типовых атак. на рис. 4 изображена обобщенная схема системы мониторинга безопасности.

Центральным элементом системы мониторинга безопасности является декодирующий анализатор протоколов. каждый декодированный пакет сравнивается с образцами атак из библиотеки сигнатур и в случае выявления сходства генерируется сигнал тревоги. В отличие от самых совершенных анализаторов протоколов, система мониторинга безопасности обладает широким спектром специализированных агентов, размещаемых на различных сетевых устройствах. существуют агенты для маршрутизаторов, для серверов, для межсетевых экранов, для систем управления базами данных и других ответственных приложений. Каждый агент обладает достаточно сложной структурой и снабжается настраиваемым фильтром, позволяющим отбирать из магистрали подозрительные с точки зрения безопасности пакеты. Системы мониторинга безопасности снабжены, как правило, средствами формализации правил политики безопасности, которые совместно с библиотеками сигнатур атак являются фундаментом процесса идентификации возможных атак.

Система мониторинга безопасности может применяться в комплексе с межсетевым экраном, выполняя при этом следующие основные задачи:

- защита от внешних угроз посредством контроля трафика, проходящего между внешней и внутренней сетями. при этом система мониторинга безопасности дополняет возможности межсетевого экрана в части фильтрации трафика.
- защита от внутренних угроз посредством контроля внутреннего трафика.

Система мониторинга безопасности обеспечивает выявление следующих типов «подозрительной» сетевой активности:

- атаки типа «отказ в услугах».
- попытки получения несанкционированного доступа.
- «подозрительные» приложения.
- сетевые игры.

Система мониторинга безопасности обеспечивает:

пассивную защиту – при обнаружении запрещенной сетевой активности система фиксирует действия в регистрационном журнале и отправляет сообщение на консоль администратора, e-mail сообщение, сообщение на пейджер;

Активную защиту - при обнаружении запрещенной сетевой активности система сбрасывает соединение с адресом, являющимся источником угрозы и модифицирует правила фильтрации межсетевого экрана (маршрутизатора) таким образом, чтобы запретить доступ с этого адреса.

Кроме того, возможна адаптация правил обнаружения запрещенной сетевой активности в соответствии с правилами политики информационной безопасности, принятыми на предприятии.

Существующие системы мониторинга способны функционировать в локальных сетях 10-100-1000 mbps. При этом наибольшими возможностями в части масштабируемости обладают системы мониторинга, использующие в качестве модулей сбора информации аппаратные реализации анализаторов трафика – в качестве примера можно привести систему cybercop, в которой применяются анализаторы sniffer фирмы network general. Причем, чрезвычайно важным с точки зрения производительности сети является то обстоятельство, что система мониторинга безопасности, в отличие от межсетевого экрана, не снижает пропускной способности сети, поскольку производит лишь наблюдение трафика, а не маршрутизацию, как это имеет место в случае использования межсетевого экрана.

Нельзя полагаться лишь на внимание системного администратора; необходимы автоматические и непрерывно действующие средства контроля состояния сети и своевременного оповещения о возможных проблемах. Любая корпоративная компьютерная сеть, даже небольшая, требует постоянного внимания к себе. Как бы хорошо она ни была настроена, насколько бы надежное ПО не было установлено на серверах и клиентских компьютерах – нельзя полагаться лишь на внимание системного администратора; необходимы автоматические и непрерывно действующие средства контроля состояния сети и своевременного оповещения о возможных проблемах. Даже случайные сбои аппаратного или программного обеспечения могут привести к весьма неприятным последствиям. Существенное замедления функционирования сетевых сервисов и служб – еще наименее неприятное из них (хотя в худших случаях и может оставаться незамеченным в течение длительных промежутков времени). Гораздо хуже, когда критично важные службы или приложения полностью прекращают функционирование, и это остается незамеченным в течение длительного времени. Типы же «критичных» служб могут быть весьма разнообразны (и, соответственно, требовать различных методов мониторинга). От корректной работы веб-серверов и серверов БД может зависеть работоспособность внутрикорпоративных приложений и важных внешних сервисов для клиентов; сбои и нарушения работы маршрутизаторов могут нарушать связь между различными частями корпорации и ее филиалами; серверы внутренней почты и сетевых мессенджеров, автоматических обновлений и резервного копирования, принт-серверы – любые из этих элементов могут страдать от программных и аппаратных сбоев.

И все же, непреднамеренные отказы оборудования и ПО – в большинстве случаев, разовые и легко исправляемые ситуации. Куда больше вреда может принести сознательные вредоносные действия изнутри или извне сети. Злоумышленники, обнаружившие «дыру» в безопасности системы, могут произвести множество деструктивных действий – начиная от простого вывода

из строя серверов (что, как правило, легко обнаруживается и исправляется), и заканчивая заражением вирусами (последствия непредсказуемы) и кражей конфиденциальных данных (последствия плачевны).

Практически все из описанных выше сценариев (и множество аналогичных), в конечном итоге, ведут к серьезным материальным убыткам: нарушению схем взаимодействия между сотрудниками, безвозвратной утере данных, потере доверия клиентов, разглашению секретных сведений и т.п. Поскольку полностью исключить возможность отказа или некорректной работы техники невозможно, решение заключается в том, чтобы обнаруживать проблемы на наиболее ранних стадиях, и получать о них наиболее подробную информацию. Для этого, как правило, применяется различное ПО мониторинга и контроля сети, которое способно как своевременно оповещать технических специалистов об обнаруженной проблеме, так и накапливать статистические данные о стабильности и других параметрах работы серверов, сервисов и служб, доступные для подробного анализа.

Ниже мы рассматриваем базовые методы мониторинга работы сети и контроля ее защищенности.

Методы мониторинга состояния сети. Выбор способов и объектов мониторинга сети зависит от множества факторов – конфигурации сети, действующих в ней сервисов и служб, конфигурации серверов и установленного на них ПО, возможностей ПО, используемого для мониторинга и т.п. На самом общем уровне можно говорить о таких элементах как:

- проверка физической доступности оборудования;
- проверка состояния (работоспособности) служб и сервисов, запущенных в сети;

- детальная проверка не критичных, но важных параметров функционирования сети: производительности, загрузки и т.п.;
- проверка параметров, специфичных для сервисов и служб данного конкретного окружения (наличие некоторых значений в таблицах БД, содержимое лог-файлов).

Начальный уровень любой проверки – тестирование физической доступности оборудования (которая может быть нарушена в результате отключения самого оборудования либо отказе каналов связи). Как минимум, это означает проверку доступности по ICMP-протоколу (ping), причем желательно проверять не только факт наличия ответа, но и время прохождения сигнала, и количество потерянных запросов: аномальные значения этих величин, как правило, сигнализируют о серьезных проблемах в конфигурации сети. Некоторые из этих проблем легко отследить при помощи трассировки маршрута (traceroute) – ее также можно автоматизировать при наличии «эталонных маршрутов».

Следующий этап – проверка принципиальной работоспособности критичных служб. Как правило, это означает TCP-подключение к соответствующему порту сервера, на котором должна быть запущена служба, и, возможно, выполнение тестового запроса (например, аутентификации на почтовом сервере по протоколу SMTP или POP или запрос тестовой страницы от веб-сервера).

В большинстве случаев, желательно проверять не только факт ответа службы/сервиса, но и задержки – впрочем, то относится уже к следующей по важности задаче: проверке нагрузки. Помимо времени отклика устройств и служб для различных типов серверов существуют другие принципиально важные проверки: память и загруженность процессора (веб-сервер, сервер БД),

место на диске (файл-сервер), и более специфические – например, статус принтеров у сервера печати.

Способы проверки этих величин варьируются, но один из основных, доступных почти всегда – проверка по SNMP-протоколу. Помимо этого, можно использовать специфические средства, предоставляемые ОС проверяемого оборудования: к примеру, современные серверные версии ОС Windows на системном уровне предоставляют так называемые счетчики производительности (performance counters), из которых можно «считать» довольно подробную информацию о состоянии компьютера.

Наконец, многие окружения требуют специфических проверок – запросов к БД, контролирующих работу некоего приложения; проверка файлов отчетов или значений настроек; отслеживание наличия некоторого файла (например, создаваемого при «падении» системы).

Контроль безопасности сети. Безопасность компьютерной сети (в смысле защищенности ее от вредоносных действий) обеспечивается двумя методами: аудитом и контролем. Аудит безопасности – проверка настройки сети (открытых портов, доступности «внутренних» приложений извне, надежности аутентификации пользователей); методы и средства аудита выходят за рамки данной статьи.

Сущность контроля безопасности состоит в выявлении аномальных событий в функционировании сети. Предполагается, что базовые методы обеспечения и контроля безопасности (аутентификация, фильтрация запросов по адресу клиента, защита от перегрузок и т.п.) встроена во все серверное ПО. Однако, во-первых, не всегда можно доверять этому предположению; во-вторых, не всегда такой защиты достаточно. Для полноценной уверенности в безопасности сети в большинстве случаев необходимо использовать дополнительные, внешние средства. При этом проверяют, как правило, следующие параметры:

- нагрузку на серверное ПО и «железо»: аномально высокие уровни загрузки процессора, внезапное сокращение свободного места на дисках, резкое увеличение сетевого трафика зачастую являются признаками сетевой атаки;

- журналы и отчеты на наличие ошибок: отдельные сообщения об ошибках в лог-файлах программ-серверов или журнале событий серверной ОС допустимы, но накопление и анализ таких сообщений помогает выявить неожиданно частые или систематические отказы;

- состояние потенциально уязвимых объектов – например, тех, «защищенность» которых тяжело проконтролировать напрямую (ненадежное стороннее ПО, изменившаяся/непроверенная конфигурация сети): нежелательные изменения прав доступа к некоторому ресурсу или содержимого файла может свидетельствовать о проникновении «врага».

Во многих случаях аномалии, замеченные при мониторинге и контроле, требуют немедленной реакции технических специалистов, соответственно, средство мониторинга сети должно иметь широкие возможности для пересылки оповещений (пересылка сообщений в локальной сети, электронной почтой, Интернет-пейджером). Изменения других контролируемых параметров реакции не требуют, но должны быть учтены для последующего анализа. Зачастую же необходимо и то, и другое – непрерывный сбор статистики плюс немедленная реакции на «выбросы»: например, отмечать и накапливать все случаи загрузки процессора более 80%, а при загрузке более 95% – немедленно информировать специалистов. Полноценный мониторинговый софт должен позволять организовывать все эти (и более сложные) сценарии.1.2. Аудит и мониторинг безопасности

Для организаций, компьютерные сети которых насчитывают не один десяток компьютеров, функционирующих под управлением различных ОС, на первое место выступает задача управления множеством разнообразных защитных механизмов в таких гетерогенных корпоративных сетях. Сложность

сетевой инфрастуктуры, многообразие данных и приложений приводят к тому, что при реализации системы информационной безопасности за пределами внимания администратора безопасности могут остаться многие угрозы. Поэтому необходимо осуществление регулярного аудита и постоянного мониторинга безопасности ИС.

Аудит безопасности информационной системы. Понятие аудита безопасности. Аудит представляет собой независимую экспертизу отдельных областей функционирования предприятия. Одной из составляющих аудита предприятия является аудит безопасности его ИС.

В настоящее время актуальность аудита безопасности ИС резко возросла. Это связано с увеличением зависимости организаций от информации и ИС. Возросла уязвимость ИС за счет повышения сложности элементов ИС, появления новых технологий передачи и хранения данных, увеличения объема ПО. Расширился спектр угроз для ИС из-за активного использования предприятиями открытых глобальных сетей для передачи сообщений и транзакций.

Аудит безопасности ИС дает возможность руководителям и сотрудникам организаций получить ответы на вопросы:

• как оптимально использовать существующую ИС при развитии бизнеса;

• как решаются вопросы безопасности и контроля доступа;

• как установить единую систему управления и мониторинга ИС;

• когда и как необходимо провести модернизацию оборудования и ПО;

• как минимизировать риски при размещении конфиденциальной информации в ИС организации, а также наметить пути решения обнаруженных проблем.

На эти и другие подобные вопросы нельзя мгновенно дать однозначный ответ. Достоверную и обоснованную информацию можно получить, только рассматривая все взаимосвязи между проблемами. Проведение аудита позволяет оценить текущую безопасность ИС, оценить риски, прогнозировать и управлять их влиянием на бизнес-процессы организации, корректно и

обоснованно подойти к вопросу обеспечения безопасности информационных ресурсов организации.

Цели проведения аудита безопасности ИС:

• оценка текущего уровня защищенности ИС;

• локализация узких мест в системе защиты ИС;

• анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;

• выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС;

• оценка соответствия ИС существующим стандартам в области информационной безопасности.

В число дополнительных задач аудита ИС могут также входить выработка рекомендаций по совершенствованию политики безопасности организации и постановка задач для ИТ персонала, касающихся обеспечения защиты информации.

Проведение аудита безопасности информационных систем. Работы по аудиту безопасности ИС состоят из последовательных этапов, которые в целом соответствуют этапам проведения комплексного ИТ аудита автоматизированной системы:

• инициирования процедуры аудита;

• сбора информации аудита;

• анализа данных аудита;

• выработки рекомендаций;

• подготовки аудиторского отчета.

Аудиторский отчет является основным результатом проведения аудита. Отчет должен содержать описание целей проведения аудита, характеристику обследуемой ИС, результаты анализа данных аудита, выводы, содержащие оценку уровня защищенности АС или соответствия ее требованиям стандартов, и рекомендации по устранению существующих недостатков и совершенствованию системы защиты.

Мониторинг безопасности системы. Функции мониторинга безопасности ИС выполняют средства анализа защищенности и средства обнаружения атак. Средства анализа защищенности исследуют настройки элементов защиты ОС на рабочих станциях и серверах, БД. Они исследуют топологию сети, ищут незащищенные или неправильные сетевые соединения, анализируют настройки МЭ.

В функции системы управления безопасностью входит выработка рекомендаций администратору по устранению обнаруженных уязвимостей в сетях, приложениях или иных компонентах ИС организации.

Использование модели адаптивного управления безопасностью сети дает возможность контролировать практически все угрозы и своевременно реагировать на них, позволяя не только устранить уязвимости, которые могут привести к реализации угрозы, но и проанализировать условия, приводящие к их появлению.

Мониторинг безопасности. Для организаций, компьютерные сети которых насчитывают не один десяток компьютеров, функционирующих под управлением различных ОС, на первое место выступает задача управления множеством разнообразных защитных механизмов в таких корпоративных сетях. Сложность сетевой инфрастуктуры, многообразие данных и приложений приводят к тому, что при реализации системы информационной безопасности за пределами внимания администратора безопасности могут остаться многие угрозы. Поэтому необходимо осуществление регулярного аудита и постоянного мониторинга безопасности IT - инфраструктры.

- защита от вирусных программ, шпионских модулей и несанкционированного доступа;
- распределение прав и контроль над доступом к ресурсам информационной системы клиента;
- учет и оптимизация затрат на использование ресурсов сети Интернет;

- создание резервных копий и восстановление ключевой информации после сбоев;
- удаленное администрирование сетей.

Преимущества мониторинга включают в себя следующие аспекты:

- снижение производственных затрат в сфере IT
- повышение производительности работы
- защита доходов клиентов
- помощь в планировании пропускной способности сети

Мониторинг позволит Вашей организации проверять доступность сервиса в режиме реального времени, проверять данные по прошедшей доступности сервиса и использовать эту информацию для соответствия уровню обслуживания, гарантированному пользователям данного приложения и Вашей организации в целом.

Средства для мониторинга сетей. Средства для мониторинга сети и обнаружения в её работе «узких мест» можно разделить на два основных класса:

• стратегические;

• тактические.

Назначение стратегических средств состоит в контроле за широким спектром параметров функционирования всей сети и решении проблем конфигурирования ЛВС. Назначение тактических средств – мониторинг и устранение неисправностей сетевых устройств и сетевого кабеля. К стратегическим средствам относятся:

• системы управления сетью

• встроенные системы диагностики

• распределённые системы мониторинга

• средства диагностики операционных систем, функционирующих на больших машинах и серверах.

Наиболее полный контроль за работой, осуществляют системы управления сетью, разработанные такими фирмами, как DEC, Hewlett – Packard, IBM и

AT&T. Эти системы обычно базируются на отдельном компьютере и включают системы контроля рабочих станций, кабельной системой, соединительными и другими устройствами, базой данных, содержащей контрольные параметры для сетей различных стандартов, а также разнообразную техническую документацию. Одной из лучших разработок для управления сетью, позволяющей администратору сети получить доступ ко всем её элементам вплоть до рабочей станции, является пакет LANDesk Manager фирмы Intel, обеспечивающий с помощью различных средств мониторинг прикладных программ, инвентаризацию аппаратных и программных средств и защиту от вирусов. Этот пакет обеспечивает в реальном времени разнообразной информацией о прикладных программах и серверах, данные о работе в сети пользователей. Встроенные системы диагностики стали обычной компонентой таких сетевых устройств, как мосты, репиторы и модемы. Примерами подобных систем могут служить пакеты Open – View Bridge Manager фирмы Hewlett – Packard и Remote Bridge Management Software фирмы DEC. К сожалению большая их часть ориентирована на оборудование какого – то одного производителя и практически несовместима с оборудованием других фирм. Распределённые системы мониторинга представляют собой специальные устройства, устанавливаемые на сегменты сети и предназначенные для получения комплексной информации о трафике, а также нарушениях в работе сети. Эти устройства, обычно подключаемые к рабочей станции администратора, в основном используются в много сегментных сетях. К тактическим средствам относят различные виды тестирующих устройств (тестеры и сканеры сетевого кабеля), а также устройства для комплексного анализа работы сети – анализаторы протоколов. Тестирующие устройства помогают администратору обнаружить неисправности сетевого кабеля и разъёмов, а анализаторы протоколов – получать информацию об обмене данными в сети. Кроме того, к этой категории средств относят специальное ПО, позволяющее в режиме реального времени получать подробные отчёты о состоянии работы сети.

Средства сетевого мониторинга

- Программа ping
- Программа ipconfig
- Серверы SNMP
- Hyperic HQ (Open Source)
- Zabbix (Open Source)
- TclMon (Open Source)
- MRTG (GNU)
- RRDtool (GNU)
- Nagios (ранее *Netsaint*) (Open Source)
- Cricket
- PRTG
- Intellipool Network Monitor
- NetDecision
- Monit (Open Source)
- Munin[1]
- GFI Webmonitor
- OpenNMS (Open Source)
- Cacti (Open Source)

ping — утилита для проверки соединений в сетях на основе TCP/IP, а также обиходное наименование самого запроса.

Первоначально словом «ping» (по созвучию) именовали направленный акустический сигнал противолодочных гидролокаторов («асдиков») времён Второй Мировой войны.

Утилита отправляет запросы (ICMP Echo-Request) протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). Время между отправкой запроса и получением ответа (RTT, от англ. *Round Trip Time*) позволяет определять двусторонние задержки (RTT) по маршруту и частоту потери пакетов, то есть косвенно определять загруженность на каналах передачи данных и промежуточных устройствах.

В разговорной речи пингом называют также время, затраченное на передачу пакета информации в компьютерных сетях от клиента к серверу и обратно от сервера к клиенту.

Программа ping является одним из основных диагностических средств в сетях TCP/IP и входит в поставку всех современных сетевых операционных систем. Функциональность ping также реализована в некоторых встроенных ОС маршрутизаторах, доступ к результатам выполнения ping для таких устройств по протоколу SNMP определяется RFC 2925 (Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations).

Так как для отправки ICMP-пакетов требуется создавать raw-сокеты, для выполнения программы ping в UNIX-системах необходимы права суперпользователя. Чтобы обычные пользователи могли использовать ping в правах доступа файла /bin/ping устанавливают SUID-бит.

Выводы по первой главе

1. Анализ проблем обеспечения информационной безопасности показывает целесообразность использования наряду со стандартными механизмами современных средств защиты компьютерных сетей: защита от внешних и внутренних угроз посредством контроля внутреннего трафика.

2. Рассмотрены методы мониторинга безопасности, решающие проблемы непрерывного контроля компьютерных сетей, обнаруживая при этом внутренние и внешние воздействие на ресурсы компьютерных сетей. Наиболее перспективными и широко используемыми методами является: декодирование и анализ сетевых пакетов, мониторинг активного сетевого оборудования, мониторинг состояния кабельной системы, мониторинг состояния серверов и ответственных рабочих станций, мониторинг приложений.

ГЛАВА 2. АНАЛИЗ СИСТЕМЫ МОНИТОРИНГА БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ.

2.1. Формальная модель защищенной компьютерной сети

Защищенность является одним из важнейших показателей эффективности функционирования компьютерных сетей (КС), наряду с такими показателями как надежность, отказоустойчивость, производительность и т. п.

Под защищенностью КС будем понимать степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации. Под угрозами безопасности информации традиционно понимается возможность нарушения таких свойств информации, как конфиденциальность, целостность и доступность.

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

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

Описанный в настоящей работе подход позволяет получать качественные оценки уровня защищенности ас путем сопоставления свойств и параметров КС с многократно опробованными на практике и стандартизированными критериями оценки защищенности.

Для того, чтобы математически точно определить этот показатель, рассмотрим формальную модель системы защиты КС.

Основой формального описания систем защиты традиционно считается модель системы защиты с полным перекрытием, в которой рассматривается взаимодействие "области угроз", "защищаемой области" (ресурсов КС) и "системы защиты" (механизмов безопасности ас).

Таким образом, имеем три множества:

t = {ti} - множество угроз безопасности,

o = {oj} - множество объектов (ресурсов) защищенной системы,

m = {mk} - множество механизмов безопасности.

Элементы этих множеств находятся между собой в определенных отношениях, собственно и описывающих систему защиты.

Для описания системы защиты обычно используется графовая модель, представленная на рисунок 2.1. множество отношений угроза-объект образует двухдольный граф {<t, o>}. цель защиты состоит в том, чтобы перекрыть все возможные ребра в графе. это достигается введением третьего набора m. в результате получается трехдольный граф {<t, m, o>}.**P**

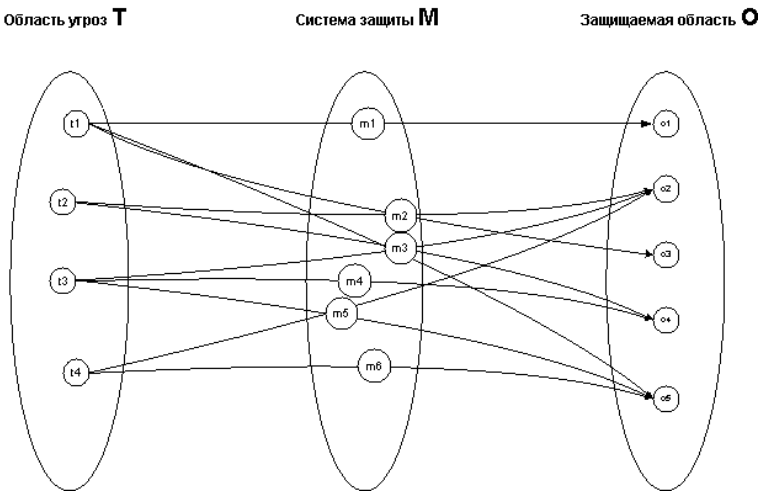


Рис. 2.1. Графовая модель системы защиты.

Развитие этой модели предполагает введение еще двух элементов:

V - набор уязвимых мест, определяемый подмножеством декартова произведения T*O: vr = <ti, oj>. Таким образом, под уязвимостью системы защиты будем понимать возможность осуществления угрозы t в отношении объекта o (На практике под уязвимостью системы защиты обычно понимают не саму возможность осуществления угрозы безопасности, а те свойства системы, которые способствуют успешному осуществлению угрозы, либо могут быть использованы злоумышленником для осуществления угрозы);

B - набор барьеров, определяемый декартовым произведением V*M: bl = <ti, oj, mk>, представляющих собой пути осуществления угроз безопасности, перекрытые средствами защиты.

В результате получаем систему, состоящую из пяти элементов: <T, O, M, V, B>, описывающую систему защиты с учетом наличия в ней уязвимостей, которая представлена на Рисунке 2.2.

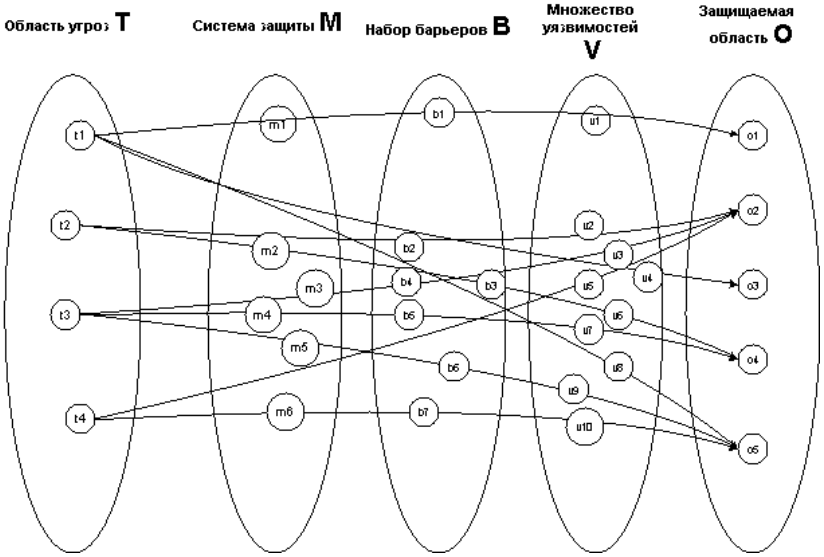


Рис.2.2.Интегрированная система безопасности

Для системы с полным перекрытием выполняется условие:

$$\forall \langle t_i, o_j \rangle \in V \; \exists \langle t_i, o_j, m_k \rangle \in B,$$

т.е. для любой уязвимости имеется соответствующий барьер, устраняющий эту уязвимость.

Интегрированная система безопасности(ИСБ) – совокупность технических средств (двух или более взаимоувязанных КС), предназначенных для

построения систем охранной, пожарной сигнализации и оповещения, управления противопожарной автоматикой, контроля и управления доступом и систем телевизионного наблюдения, которые обладают технической, информационной, программной и эксплуатационной совместимостью так, что эту совокупность можно рассматривать как единую КС.

Из этого определения также следует, что ИСБ это система, обеспечивающая защиту от нескольких видов угроз. В данном выше определении – ИСБ предназначена для защиты от пожара (пожарная сигнализация, оповещение, противопожарная автоматика) и от криминальных угроз (охранная сигнализация, контроль доступа, охранное телевидение).

Современные ИСБ строятся на основе иерархической сетевой структуры, в которую входят компьютерные сети, а также локальные сети различного уровня сложности специальных вычислительных устройств - контроллеров.

Обобщенная структура ИСБ приведена на рисунке 2.3. В ней можно выделить четыре уровня сетевого взаимодействия

Первый (верхний) уровень представляет собой компьютерную сеть типа клиент/сервер на основе сети Ethernet, с протоколом обмена TCP/IP и с использованием сетевых операционных систем. Этот уровень обеспечивает связь между сервером и рабочими станциями операторов. Управление ИСБ на верхнем уровне обеспечивается посредством специализированного программного обеспечения (СПО). Для небольших объектов возможно использование для управления ИСБ одного компьютера. На верхнем уровне также обеспечивается связь и управление удаленными объектами. Современные возможности компьютерных сетей позволяют передавать информацию по различным каналам связи, тем самым на основе ИСБ можно создавать системы мониторинга безопасности удаленных объектов.

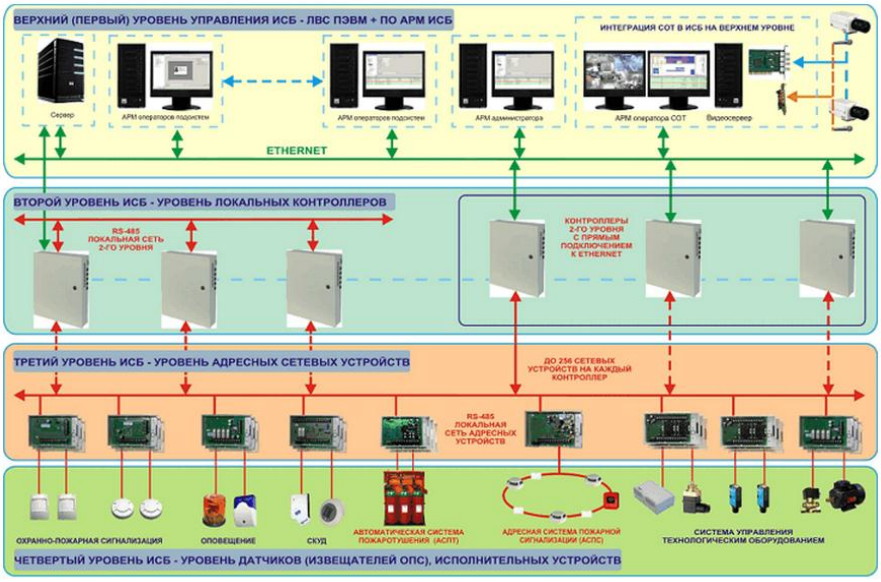


Рис.2.3. Интегрированная система безопасности

Второй уровень – уровень локальных контроллеров, основных компонентов управления ИСБ. Каждый локальный контроллер должен обеспечивать выполнение основных функций в своей зоне контроля, даже при нарушении связи с верхним уровнем ИСБ. Для связи между однородными контроллерами (горизонтальный уровень связи) используется интерфейс RS485 или другие интерфейсы, предназначенные для построения сетей промышленного уровня с хорошей помехозащищенностью и достаточной скоростью обмена данными. Связь между вторым и верхним уровнем (вертикальный уровень связи) может обеспечиваться через один из сетевых контроллеров, посредством подключения его к серверу ПО АРМ ИСБ через стандартный порт ПЭВМ. В контроллерах некоторых ИСБ возможен прямой выход на первый уровень в протоколе TCP/IP.

Третий уровень – уровень адресных сетевых устройств, которые подключаются к каждому контроллеру второго уровня. Здесь, как правило, применяется интерфейс RS485. Количество сетевых устройств, подключаемых к одному контроллеру, может быть до 256. Номенклатура адресных сетевых устройств достаточно разнообразна, от простых расширителей для подключения радиальных ШС до сложных контроллеров третьего уровня,

например, устройств управления пожаротушением или модулей подключения адресно-аналоговах пожарных извещателей.

Четвертый уровень – извещатели и оповещатели ОПС, считыватели и исполнительные устройства СКУД, датчики и устройства управления технологическим оборудованием и др.. Здесь, как правило, применяются нестандартные специализированные интерфейсы и протоколы.

Технические возможности ИСБ позволяют определить дальнейшие перспективы их развития – интеграция с другими системами автоматизации и расширение видов и количества угроз, защита от которых обеспечивается с помощью ИСБ.

Тенденция дальнейшей интеграции – объединение ИСБ с системами автоматизации и управления инженерными системами здания или объекта связана с появлением термина – «интеллектуальное здание».

2.2. Анализ аппаратно-программных средств мониторинга защищенности корпоративных сетей

При создании информационной инфраструктуры корпоративной автоматизированной системы (АС) на базе современных компьютерных сетей неизбежно возникает вопрос о защищенности этой инфраструктуры от угроз безопасности информации.

Компания LETA в рамках Услуги «Оценка защищенности ресурсов сети» предлагает два варианта внедрения и выполнения работ:

Разовая оценка защищенности. Специалисты компании LETA с помощью выбранного Заказчиком технического средства выполняют разовое сканирование корпоративной сети согласно заданным параметрам.

По результатам работы подготавливается отчет о результатах сканирования, который содержит результаты проведенных работ по выявлению уязвимостей корпоративной сети Заказчика, а также экспертные заключения специалистов LETA и рекомендации по результатам сканирования.

Внедрение системы управления уязвимостями. Специалисты Исполнителя обеспечивают внедрение системы управления уязвимостями на стороне Заказчика, что позволяет значительно повысить защищенность всей информационной системы в целом и вывести ИБ в организации на качественно новый уровень.

Внедрение системы управления уязвимостями позволяет:

- автоматизировать управление жизненным циклом уязвимостей;
- регламентировать процессы обнаружения, анализа и устранения уязвимостей;
- обеспечить четкий алгоритм устранения обнаруженных в результате сканирования уязвимостей, в приоритетном порядке на основе критичности тех или иных обнаруженных уязвимостей;
- поддерживать в актуальном состоянии высокую степень защищенности корпоративной сети.

Состав внедряемой системы управления уязвимостями:

решение по управлению уязвимостями – сканирование внешних и внутренних ip-адресов корпоративной сети, выявление уязвимостей, их анализ и устранение;

соответствие политикам безопасности – автоматическая проверка на соответствие требованиям политик безопасности, рекомендаций и стандартов (PCI DSS, COBIT, ISO,SOX, Basel II и др.);

Контроль защищенности веб-приложений – выявление, анализ и устранение уязвимостей, присущих именно веб-приложениям (SQL-injection, XSS и др.);

организационно-распорядительная документация – набор документов, обеспечивающих регламентирование процесса управления уязвимостями в рамках корпоративной сети, в общем случае включает в себя политику управления уязвимостями, процедуры проведения сканирований и устранения уязвимостей, а также различные инструкции и другие документы.

Обеспечение выполнения внутренних и внешних требований, а также оценка эффективности имеющихся мер контроля являются основными задачами процесса внутреннего аудита ИБ. Компания LETA предлагает набор услуг, направленных на формирование четких требований ИБ в организации и успешное обеспечение контроля за их выполнением.куда входят:

- оценка соответствия информационной системы Заказчика установленным внешним или внутренним требованиям;
- разработка политик и стандартов в области ИБ;
- разработка и внедрение процедур внутреннего аудита ИБ:
- сбор и анализ информации;
- определение актуальных требований;
- оценка рисков;
- оценка эффективности имеющихся мер контроля;
- анализ со стороны руководства;
- внедрение корректирующих мер по итогам аудита;
- проектирование и внедрение программно-технических средств аудита и контроля за соответствием требованиям;
- разработка технических проверок для информационных систем Заказчика;
- консультационное сопровождение и техническая поддержка.

Что дает внедрение услуги по построению системы внутреннего аудита и обеспечения соответствия требованиям политик ИБ

Предлагаемые программно-технические решения позволяют значительно снизить трудозатраты на выполнение процедур внутреннего аудита ИБ за счет автоматизации процесса, а также существенно повысить полноту и качество собираемой информации.

Комплексная система МСР.Система.0.7 предоставляет услуги связи с использованием стационарных, мобильных и персональных программно-аппаратных комплексов на основе специальной сети передачи данных (ССПД) ОАО «Мегафон» для развертывания полноценной сети по классу

защищенности 1Г, без доступа в Интернет, с возможностью масштабирования от предприятия до всей территории РФ, с обменом конфиденциальной информацией (речь, видео, данные) с помощью мобильного комплекса МК-СУ-01 и персонального МСР-Терминала.

Основные функции МСР.Системы 0.7:1. Формирование федеральных и региональных разнородных баз данных по объектам учета, управления и мониторинга.2. Ведение единого реестра паспортов объектов.3. Оперативный доступ к БД объектов с любой точки РФ с применением мобильных персональных терминалов.4. Ведение и пополнение разнородных БД с оперативным доступом к паспортам объектов, текущим технико-экономическим показателям, нормативным документам в автоматизированном и ручном режимах.5. Автоматизированное составление и выдача формализованных данных в виде документов, таблиц и графиков.

Система позволяет:

- осуществлять мониторинг местоположения абонентов с использованием СНС ГЛОНАСС/GPS и по технологии Cell ID по активной соте GSM;
- производить оповещение и управление абонентами голосом и текстовыми сообщениями (SMS);
- организовать службу информации (CellBroadcast GSM);
- организовать закрытые группы абонентов с короткими номерами и выходом на фиксированную связь;
- использовать единый тарифный план на всей территории РФ и IP-адресацию заказчика;

Комплексная система МСР.Система.07 состоит из мобильного оборудования **МСР-МКУ СУ** со специальным программным обеспечением для доступа к базам данных, мониторинга состояния сети, систем НСД и СКЗИ для обеспечения безопасности и базируется на *специальных услугах связи*, предоставляемых оператором сотовой связи **GSM ОАО «МегаФон»**, которые включают в себя:

- услуги специальной сети передачи данных (ССПД) с обеспечением приоритетного обслуживания, в том числе и радиоинтерфейсе;
- услуги специальной федеральной подсистемы конфиденциальной сотовой связи (СФПКСС) со специальными сотовыми телефонами;
- услуги конвергированной фиксированной мобильной связи (ФМС);
- услуги стандартных сервисов сотовой связи GSM (АОП, короткие номера, MMS, SMS, пакетная передача данных GPRS, конференц-связь и т.д.

Использование Alchemy Eye для мониторинга состояния сети и контроля ее безопасности. Alchemy Eye – средство мониторинга состояния серверов в сети с богатыми возможностями. Ниже показано, как реализуются сценарии, описанные в предыдущих разделах, посредством этой программы.

Прежде всего, чтобы обеспечить непрерывность мониторинга, нужно запустить программу как NT-службу (установить ее в Файл>Настройки>NT-служба, затем запустить из Панели управления Windows). После запуска службы появится иконка в области уведомлений (системном трее), по клику на ней откроется главное окно программы, где и нужно создать необходимые проверки.

Alchemy Eye позволяет создавать любое количество *объектов мониторинга* («сервер» в терминах программы, но пусть это вас не смущает: одному физическому серверу может соответствовать любое количество объектов мониторинга). Каждому объекту мониторинга соответствует проверка одного типа для одного компьютера.

Чтобы добавить проверку в программ, откройте диалог создания нового сервера (меню «Сервер>Добавить сервер>Новый») – рис 2.4. На основной закладке этого диалога нужно задать логическое имя для объекта мониторинга, интервал между проверками, и тип проверки.

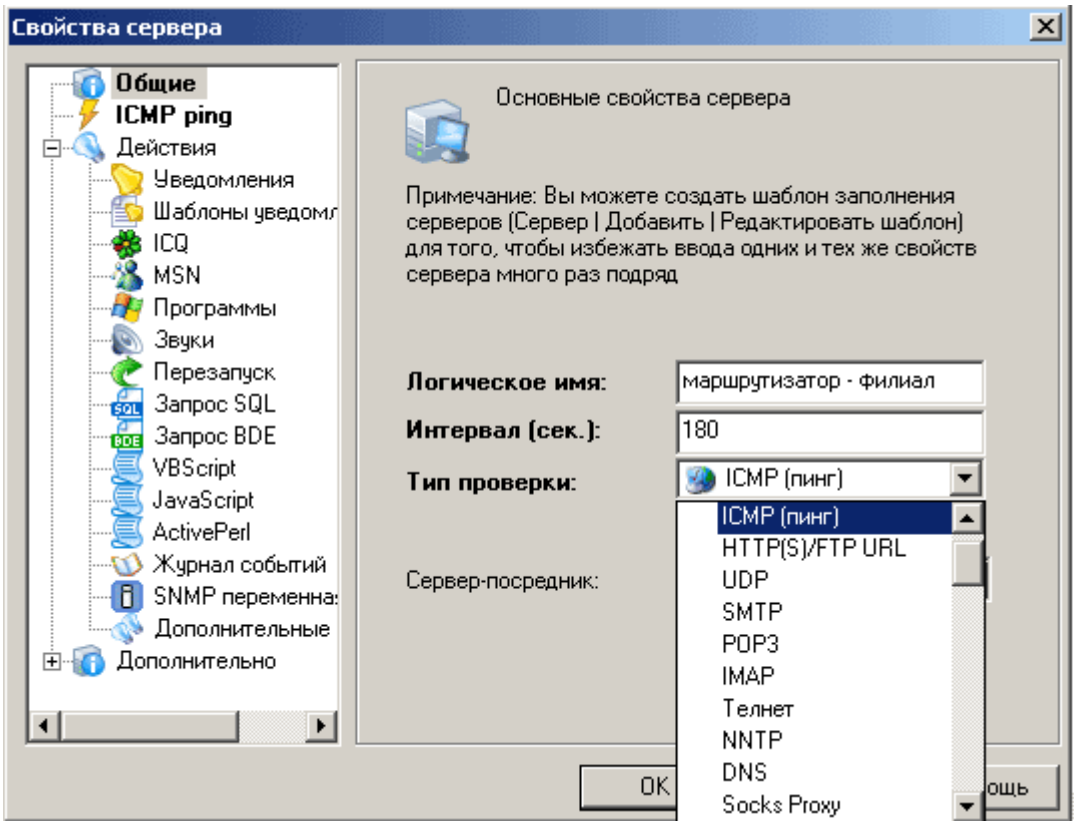


Рис.2.4. Выбор типа проверки сервера.

Скриншот на рис.2.4. может продемонстрировать лишь небольшое количество типов проверок, доступных в программе (полный список вы можете посмотреть самостоятельно). Для ориентировки можно привести соответствия между задачами, описанными выше, и некоторыми проверками, доступными в Alchemy Eye:

- **Проверка физической доступности оборудования**: ICMP, UDP, трассировка маршрута (traceroute).
- **Проверка работоспособности служб и сервисов**, запущенных в сети: все стандартные протоколы (POP/SMTP, DNS, DHCP,HTTP/FTP), подключение к базам данных (Oracle, MySQL, MS SQL Server, или любая БД, доступная через источники данных ODBC). Кроме того, Alchemy Eye предоставляет мощное средство для проверки нестандартных серверов – TCP-скрипт. В этой проверке можно описать достаточно сложную логику подключения к порту сервера, отсылки ему любых строк-команд и тестирования ответов.
- **Проверка нагрузки сети и отдельных служб**: можно использовать проверку стандартных переменных SNMP MIB (Management Information Base) –

программа не только позволяет контролировать их, но и предоставляет дерево-список всех доступных в MIB переменных (рис.2.5). Счетчики производительности для Windows-машин доступны «из коробки» (рис. 3), а сходная функциональность для **nix-серверов – в виде бесплатного плагина на сайте производителя.**

- Проверка специфических параметров* для данного окружения: список проверок включает и SQL-запросы с проверкой результата, и анализ лог-файлов (в том числе на удаленных компьютерах), и еще более специфичные проверки (например, анализ значений ключей реестра или журнала событий Windows).
- Проверка состояния уязвимых объектов: сюда можно отнести подключение по TCP/IP к любому порту удаленного компьютера, проверка прав доступа к различным файлам и папкам (права могут быть изменены злоумышленником или некачественным ПО), проверка количества файлов в определенной папке и сравнения файла по содержимому с эталоном.

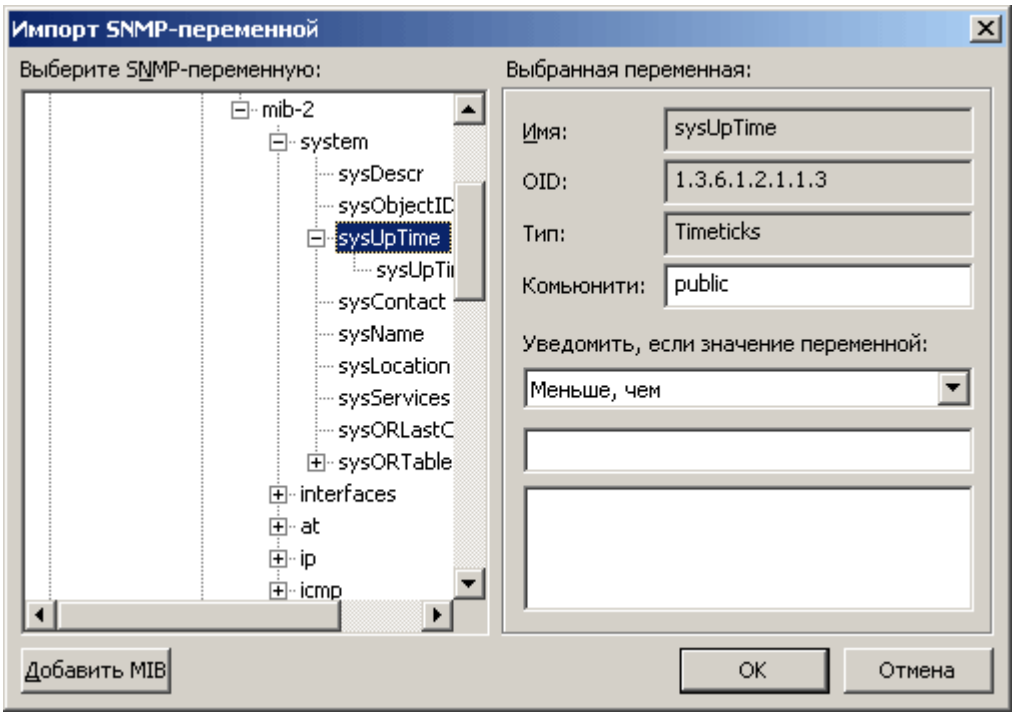


Рис.2.5. Браузер дерева MIB – выбор переменной для SNMP-мониторинга.

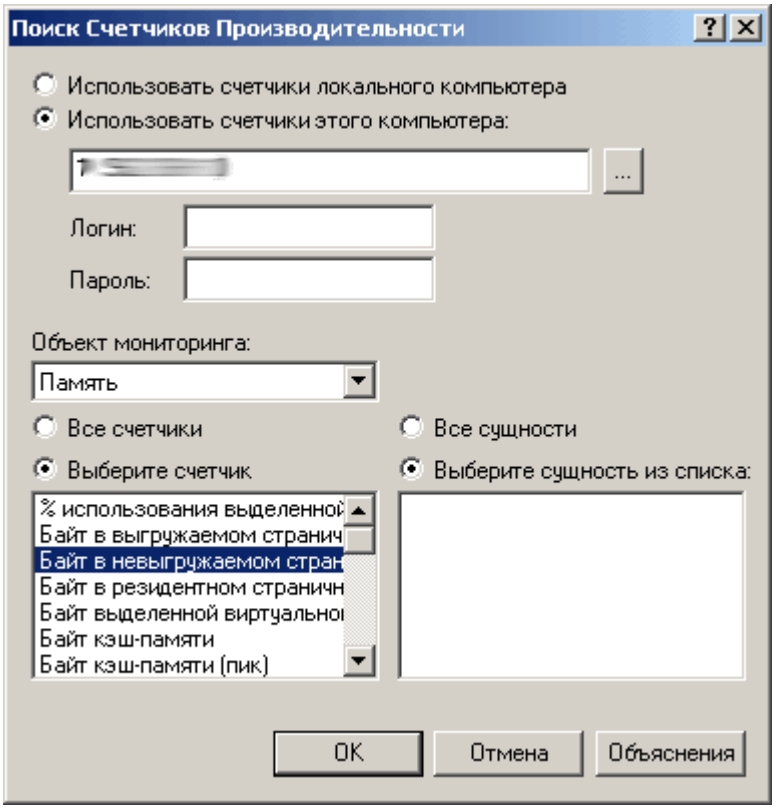


Рис.2.6. Браузер счетчиков производительности Windows – выбор параметра для мониторинга.

В случае сложных окружений, для которых недостаточно встроенных проверок, можно использовать одну из возможностей расширения, доступных в Alchemy Eye: запуск скриптовых функций (VBScript, JavaScript, ActivePerl) или внешних приложений, а так же подсистему плагинов.

После выбора типа проверки нужно задать ее параметры – как правило, они включают адрес проверяемого сервера и несколько других, очевидных либо в деталях объясняемых всплывающими подсказками. На рис.2.7. показана страница выбора параметров ICMP-проверки.

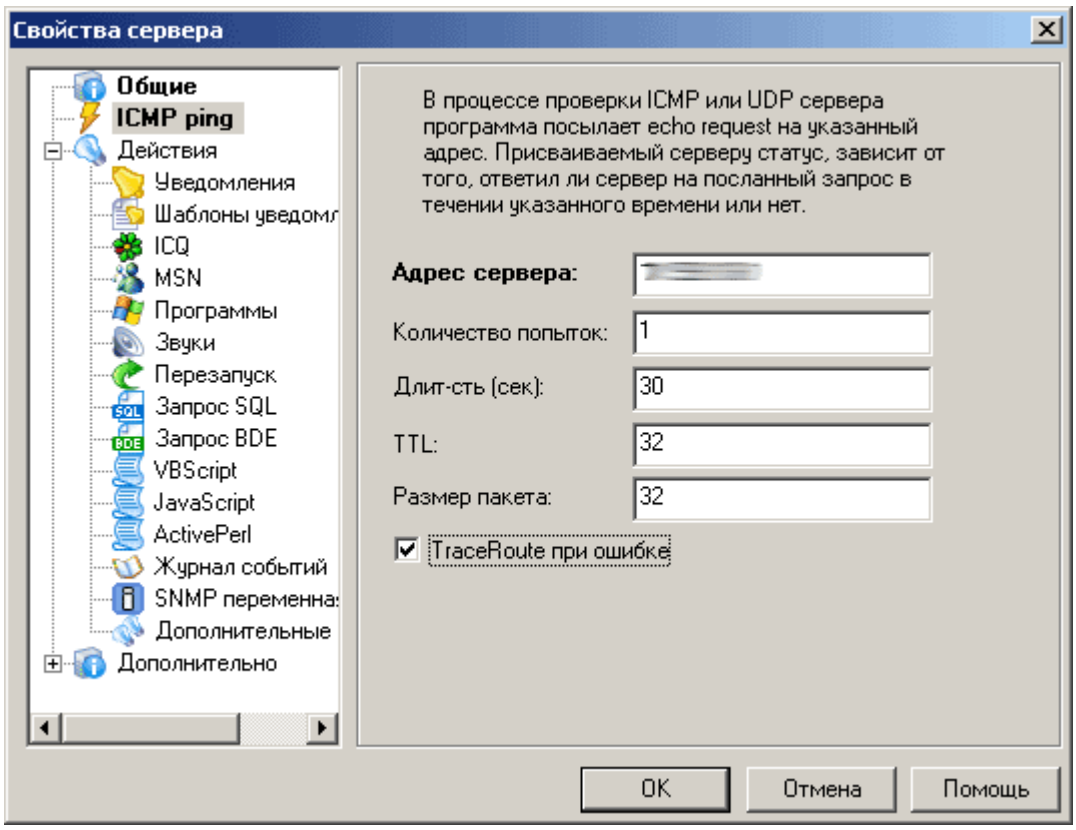


Рис.2.7. Страница выбора параметров ICMP-проверки

Если проверка является критичной (ее несрабатывание требует немедленного внимания технических специалистов), в этом же диалоге необходимо настроить уведомления: Alchemy Eye может отсылать их с помощью электронной почты, ICQ/MSN (обратите внимание, что в настройках программы должен быть настроен доступ к соответствующим аккаунтам) или сообщениями локальной сети (net send).

Когда объекты мониторинга созданы, главное окно Alchemy Eye само по себе становится инструментом анализа текущей ситуации, наглядно отображая состояния серверов (рис.2.8). Если заданных проверок больше чем 4-5 (и к тому же, они имеют разную степень критичности), лучше всего разбить их по папкам (впоследствии это даст дополнительные «приятности», вроде возможности сгенерировать отчеты только для проверок из конкретной папки).

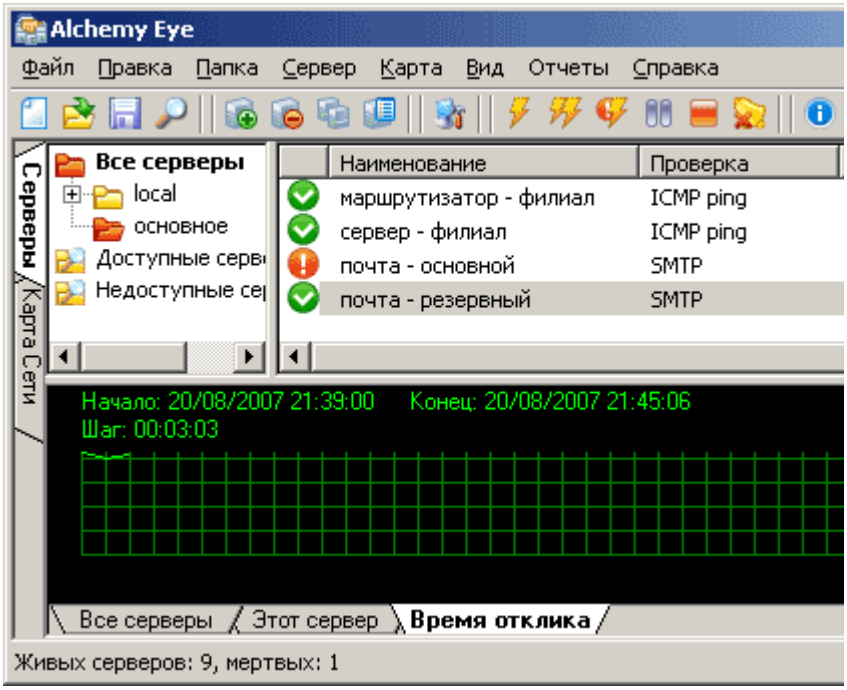


Рис.2.8. Главное окно Alchemy Eye – мониторинг серверов (3 успешных проверки,1 сбой).

Все проверки Alchemy Eye «бинарные» (проверка либо прошла, либо нет), но на количество однотипных проверок никаких ограничений не накладывается. Таким образом, встроенных средств программы вполне достаточно для реализации сложных сценариев: например, две независимые проверки загрузки процессора одного и того же сервера – одна будет «ловить» загрузку выше 95% и немедленно сообщать о проблеме техническим специалистам, а другая – загрузку выше 80% для статистического учета и последующего анализа.

Задачи этого рода (учет и анализ) в Alchemy Eye решаются с помощью встроенных отчетов (меню Отчеты). Стоит учесть, что вся статистика выполненных программой проверок и их результатов записывается в стандартной форме в файл stat.csv в папке программы, данные из него можно использовать для последующего анализа (Alchemy Eye позволяет подключать сторонние программы-анализаторы в качестве генераторов отчетов – подробная инструкция имеется в справке программы).

Напоследок хотелось бы заметить, что даже при наличии качественного программного средства разработка работающей системы мониторинга крупной

сети и контроля ее безопасности (читай – выбор необходимого количества и типов проверок) является серьезной инженерной задачей, требующей вдумчивого подхода. Две основных цели, о которых не следует забывать при конфигурации системы мониторинга:

1. создать достаточное количество проверок для обеспечения высокой степени надежности;

2. не слишком увлечься количеством и частотой проверок, чтобы избежать перегрузок оборудования, но в первую очередь – специалистов, в чьи обязанности входит анализ результатов мониторинга.

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

настройка правил разграничения доступа (правил фильрации сетевых пакетов) на МЭ и маршрутизаторах;

- используемые схемы и настройка параметров аутентификации;
- настройка параметров системы регистрации событий;
- использование механизмов, обеспечивающих сокрытие топологии защищаемой сети, включающих в себя трансляцию сетевых адресов (NAT), маскарадинг и использование системы split DNS;
- настройка механизмов оповещения об атаках и реагирования;
- наличие и работоспособность средств контроля целостности;
- версии используемого ПО и наличие установленных пакетов программных коррекций.

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

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

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

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

Средства анализа защищенности. Арсенал программных средств, используемых для анализа защищенности КС достаточно широк. Причем, во многих случаях, свободно распространяемые программные продукты ничем не уступают их коммерческим аналогам. Достаточно сравнить некоммерческий сканер NESSUS с его коммерческими аналогами.

Удобным и мощным средством анализа защищенности ОС является рассматриваемый ниже свободно распространяемый программный продукт CIS Windows 2000 Level I Scoring Tool, а также аналогичные средства разработчиков ОС, предоставляемые бесплатно, такие как ASET для ОС Solaris или MBSA (Microsoft Security Baseline Analyzer) для ОС Windows 2000.

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

Другим широко используемым методом анализа защищенности является активное тестирование механизмов защиты путем эмуляции действий злоумышленника по осуществлению попыток сетевого вторжения в АС. Для этих целей применяются сетевые сканеры, эмулирующие действия потенциальных нарушителей. В основе работы сетевых сканеров лежит база данных, содержащая описание известных уязвимостей ОС, МЭ, маршрутизаторов и сетевых сервисов, а также алгоритмов осуществления попыток вторжения (сценариев атак). Рассматриваемые ниже сетевые сканеры Nessus и Symantec NetRecon являются достойными представителями данного класса программных средств анализа защищенности.

Таким образом, программные средства анализа защищенности условно можно разделить на два класса. Первый класс, к которому принадлежат сетевые сканеры, иногда называют средствами анализа защищенности сетевого уровня. Второй класс, к которому относятся все остальные рассмотренные здесь средства, иногда называют средствами анализа защищенности системного уровня. Данные классы средств имеют свои достоинства и недостатки и на практике взаимно дополняют друг друга.

Для функционирования сетевого сканера необходим только один компьютер, имеющий сетевой доступ к анализируемым системам, поэтому, в отличие от продуктов, построенных на технологии программных агентов, нет необходимости устанавливать в каждой анализируемой системе своего агента (своего для каждой ОС).

К недостаткам сетевых сканеров можно отнести большие временные затраты, необходимые для сканирования всех сетевых компьютеров из одной системы, и создание большой нагрузки на сеть. Кроме того, в общем случае, трудно отличить сеанс сканирования от действительных попыток осуществления атак. Сетевыми сканерами также с успехом пользуются злоумышленники.

Системы анализа защищенности, построенные на интеллектуальных программных агентах, являются потенциально более мощным средством, чем сетевые сканеры. Однако, несмотря на все свои достоинства, использование программных агентов не может заменить сетевого сканирования, поэтому эти средства лучше применять совместно. Кроме того, сканеры являются более простым, доступным, дешевым и, во многих случаях, более эффективным средством анализа защищенности.

Средства анализа параметров защиты (Security Benchmarks). Уровень защищенности компьютерных систем от угроз безопасности определяется многими факторами. При этом одним из определяющих факторов является адекватность конфигурации системного и прикладного ПО, средств защиты информации и активного сетевого оборудования существующим рискам.

Перечисленные компоненты АС имеют сотни параметров, значения которых оказывают влияние на защищенности системы, что делает их ручной анализ трудновыполнимой задачей. Поэтому в современных АС для анализа конфигурационных параметров системного и прикладного ПО, технических средств и средств защиты информации зачастую используются специализированные программные средства.

Анализ параметров защиты осуществляется по шаблонам, содержащим списки параметров и их значений, которые должны быть установлены для обеспечения необходимого уровня защищенности. Различные шаблоны, определяют конфигурации для различных программно-технических средств.

Относительно коммерческих корпоративных сетей, подключенных к сети Интернет, можно говорить о некотором базовом уровне защищенности, который в большинстве случаев можно признать достаточным. Разработка спецификаций (шаблонов) для конфигурации наиболее распространенных системных программных средств, позволяющих обеспечить базовых уровень защищенности, в настоящее время осуществляется представителями международного сообщества в лице организаций и частных лиц, профессионально занимающихся вопросами информационной безопасности и аудита АС, под эгидой международной организации Центр Безопасности Интернет (Center of Internet Security). На данный момент закончены, либо находятся в разработке следующие спецификации (Security Benchmarks):

Solaris (Level-1)

Windows 2000 (Level-1)

CISCO IOS Router (Level-1/Level-2)

Linux (Level-1)

HP-UX (Level-1)

AIX (Level-1)

Check Point FW-1/VPN-1 (Level-2)

Apache Web Server (Level-2)

Windows NT (Level-1)

Windows 2000 Bastion Host (Level-2)

Windows 2000 Workstation (Level-2)

Windows IIS5 Web Server (Level-2)

В приведенном списке спецификации первого уровня (Level-1) определяют базовый (минимальный) уровень защиты, который требуется обеспечить для большинства систем, имеющих подключения к Интернет. Спецификации второго уровня (Level-2) определяют продвинутый уровень защиты, необходимый для систем, в которых предъявляются повышенные требования по безопасности.

Перечисленные спецификации являются результатом обобщения мирового опыта обеспечения информационной безопасности.

Для анализа конфигурации компонентов КС на соответствие этим спецификациям используются специализированные тестовые программные средства (CIS-certified scoring tools).

В качестве примера, рассмотрим спецификацию базового уровня защиты для ОС MS Windows 2000 и соответствующий программный инструментарий для анализа конфигурации ОС.

Windows 2000 Security Benchmark. CIS Windows 2000 Security Benchmark является программой, позволяющей осуществлять проверку соответствия настроек ОС MS Windows 2000 минимальному набору требований безопасности, определяющих базовый уровень защищенности, который, в общем случае, является достаточным для коммерческих систем. Требования к базовому уровню защищенности ОС Windows 2000 были выработаны в результате обобщения практического опыта. Свой вклад в разработку этих спецификаций внесли такие организации, как SANS Institute, Center for Internet Security, US NSA и US DoD.

В состав инструментария CIS Windows 2000 Security Benchmark входит шаблон политики безопасности (cis.inf), позволяющий осуществлять сравнение текущих настроек ОС с эталонными и производить автоматическую

переконфигурацию ОС для обеспечения соответствия базовому уровню защищенности, задаваемому данным шаблоном.

CIS Windows 2000 Security Benchmark позволяет осуществлять количественную оценку текущего уровня защищенности анализируемой ОС по 10-бальной шкале. Уровень 0 соответствует минимальному уровню защищенности (после установки ОС, ее уровень защищенности как раз и будет равен 0). Уровень 10 является максимальным и означает полное соответствие анализируемой системы требованиям базового уровня защищенности для коммерческих систем.

Сетевые сканеры. Основным фактором, определяющим защищенность АС от угроз безопасности, является наличие в АС уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов АС, так и другими причинами, в число которых входят ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их неправильное использование, либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты АС, в конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости.

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

Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers)

использовавшиеся с начала 80-х и не потерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования.

Современный сетевой сканер выполняет четыре основные задачи:

- идентификация доступных сетевых ресурсов
- идентификация доступных сетевых сервисов
- идентификация имеющихся уязвимостей сетевых сервисов
- выдача рекомендаций по устранению уязвимостей

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

Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит, таких как host, showmount, traceout, rusers, finger, ping и т. п. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

В настоящее время, существует большое количество как коммерческих, так и свободно распространяемых сканеров, как универсальных, так и специализированных - предназначенных для выявления только определенного класса уязвимостей. Многие из них можно найти в сети Интернет. Число уязвимостей в базах данных современных сканеров медленно но уверенно приближается к 1000.

Одним из наиболее продвинутых коммерческих продуктов этого класса является сетевой сканер NetRecon компании Symantec, база данных которого содержит около 800 уязвимостей UNIX, Windows и NetWare систем и

постоянно обновляется через Web. Рассмотрение его свойств позволит составить представление обо всех продуктах этого класса.

Сетевой сканер NetRecon. Сетевой сканер NetRecon является инструментом администратора безопасности, предназначенным для исследования структуры сетей и сетевых сервисов и анализа защищенности сетевых сред. NetRecon позволяет осуществлять поиск уязвимостей в сетевых сервисах, ОС, МЭ, маршрутизаторах и других сетевых компонентов. Например, NetRecon позволяет находить уязвимости в таких сетевых сервисах, как ftp, telnet, DNS, электронная почта, Web-сервер и др. При этом проверяются версии и конфигурации сервисов, их защищенность от сетевых угроз и устойчивость к попыткам проникновения. Для поиска уязвимостей используются как стандартные средства тестирования и сбора информации о конфигурации и функционировании сети, так и специальные средства, которые реализуют алгоритмы, эмулирующие действия злоумышленника по осуществлению сетевых атак.

Программа работает в среде ОС Windows NT и имеет удобный графический интерфейс, позволяющий определять параметры сканирования, наблюдать за ходом сканирования, генерировать и просматривать отчеты о результатах сканирования. Результаты отображаются в графической и в табличной форме в реальном масштабе времени.

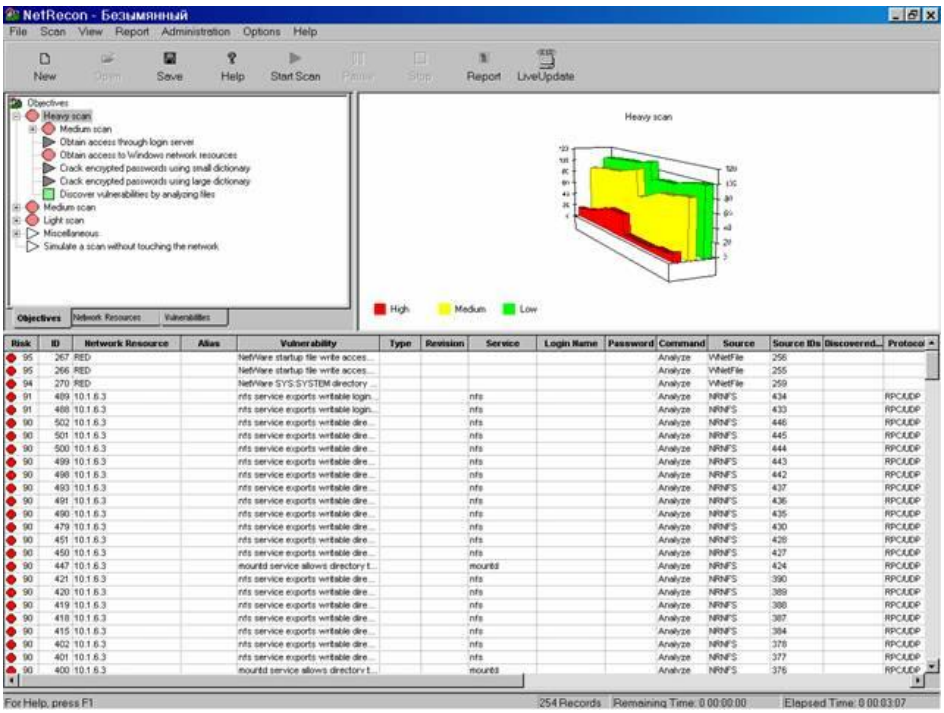


Рис.2.9. Сетевой сканер NetRecon

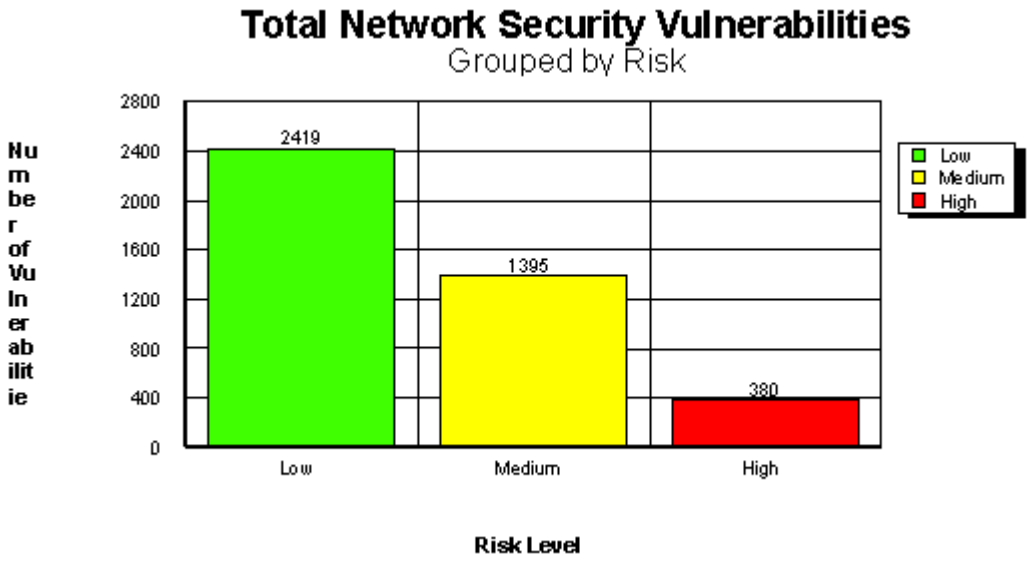


Рис.2.10. Суммарное количество уязвимостей, обнаруженных сканером NetRecon

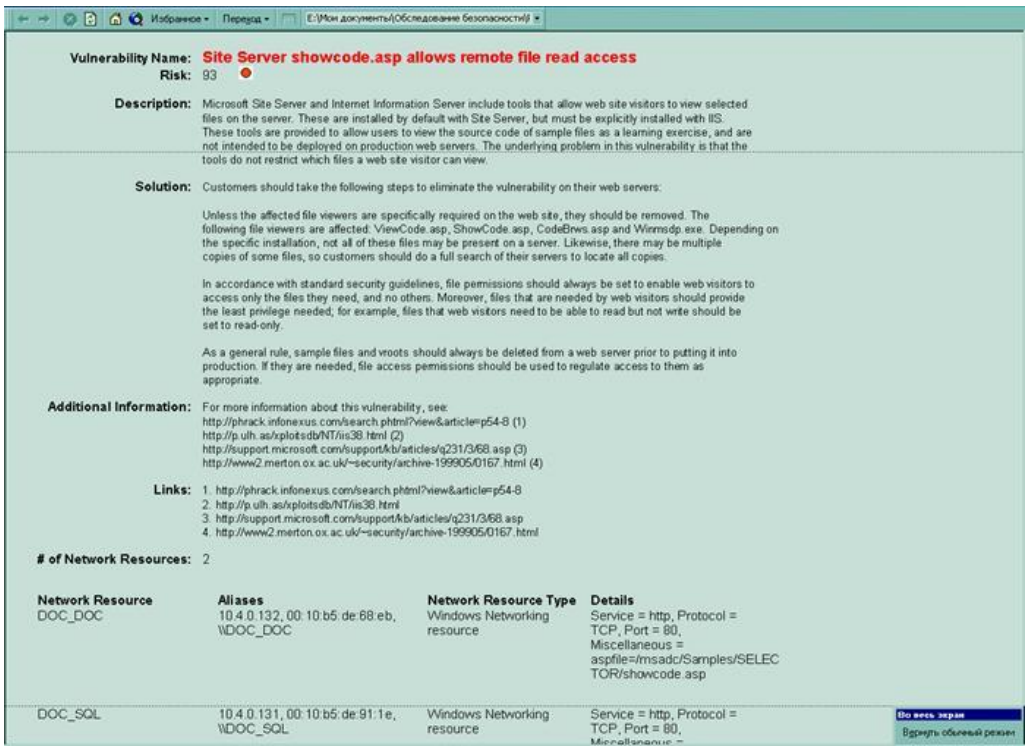
Создаваемые NetRecon отчеты содержат подробную информацию о найденных уязвимостях, включая слабость паролей пользователей, подверженность определенных сервисов угрозам отказа в обслуживании, уязвимые для сетевых атак конфигурации ОС и многие другие. Наряду с сообщениями о найденных уязвимостях и их описаниями, приводятся

рекомендации по их устранению. Отчет о результатах сканирования позволяет наметить план мероприятий по устранению выявленных недостатков.

Для генерации отчетов в NetRecon используется ПО Crystal Report, предоставляющее удобные средства для просмотра отчетов и их экспорта во все популярные форматы представления данных. Найденные уязвимости ранжируются, при этом каждой из них присваивается числовой рейтинг, что позволяет отсортировать их по степени критичности для облегчения последующего анализа результатов сканирования.

Пример описания уязвимости в отчете, сгенерированном сканером NetRecon, приведен на Рисунок 2.11. В NetRecon используется следующий формат описания уязвимости (который однако является общим и для всех остальных сетевых сканеров):

- Vulnerability Name (Название уязвимости)
- Risk (Уровень риска)
- Description (Описание уязвимости)
- Solution (Способы ликвидации уязвимости)
- Additional Information (Дополнительная информация)
- Links (Ссылки на источники информации о данной уязвимости)
- # of Network Resources (Кол-во сетевых ресурсов, подверженных данной уязвимости)
- Network Resource (Список сетевых ресурсов)



Vulnerability Name: Site Server showcode.asp allows remote file read access
Risk: 93

Description: Microsoft Site Server and Internet Information Server include tools that allow web site visitors to view selected files on the server. These are installed by default with Site Server, but must be explicitly installed with IIS. These tools are provided to allow users to view the source code of sample files as a learning exercise, and are not intended to be deployed on production web servers. The underlying problem in this vulnerability is that the tools do not restrict which files a web site visitor can view.

Solution: Customers should take the following steps to eliminate the vulnerability on their web servers:

Unless the affected file viewers are specifically required on the web site, they should be removed. The following file viewers are affected: ViewCode.asp, ShowCode.asp, CodeBrws.asp and Winmsdp.exe. Depending on the specific installation, not all of these files may be present on a server. Likewise, there may be multiple copies of some files, so customers should do a full search of their servers to locate all copies.

In accordance with standard security guidelines, file permissions should always be set to enable web visitors to access only the files they need, and no others. Moreover, files that are needed by web visitors should provide the least privilege needed; for example, files that web visitors need to be able to read but not write should be set to read-only.

As a general rule, sample files and vroots should always be deleted from a web server prior to putting it into production. If they are needed, file access permissions should be used to regulate access to them as appropriate.

Additional Information: For more information about this vulnerability, see:
http://phrack.infonexus.com/search.phtml?view&article=p54-8 (1)
http://p.ulh.as/xploitsdb/NT/iis38.html (2)
http://support.microsoft.com/support/kb/articles/q231/3/68.asp (3)
http://www2.merton.ox.ac.uk/~security/archive-199905/0167.html (4)

Links:
1. http://phrack.infonexus.com/search.phtml?view&article=p54-8
2. http://p.ulh.as/xploitsdb/NT/iis38.html
3. http://support.microsoft.com/support/kb/articles/q231/3/68.asp
4. http://www2.merton.ox.ac.uk/~security/archive-199905/0167.html

# of Network Resources: 2

Network Resource	Aliases	Network Resource Type	Details
DOC_DOC	10.4.0.132, 00:10:b5:de:68:eb, \\DOC_DOC	Windows Networking resource	Service = http, Protocol = TCP, Port = 80, Miscellaneous = aspfile=/msadc/Samples/SELECTOR/showcode.asp
DOC_SQL	10.4.0.131, 00:10:b5:de:91:1e, \\DOC_SQL	Windows Networking resource	Service = http, Protocol = TCP, Port = 80,

Рис.2.11. Описание уязвимости в отчете, сгенерированном сканером NetRecon

NetRecon самостоятельно определяет конфигурацию сети и позволяет выбрать сетевые ресурсы для сканирования. Может осуществляться параллельное сканирование всех сетевых ресурсов, сканирование по диапазону сетевых адресов, сканирование отдельных систем или подсетей. Сеанс сканирования может включать в себя все виды проверок, либо отдельные проверки по выбору пользователя. Глубина сканирования определяется продолжительностью сеанса сканирования, которая задается пользователем. Например, проверки, связанные с подбором пользовательских паролей по словарю, сопряжены с существенными временными затратами и не могут быть завершены в течение короткого сеанса сканирования.

Для поиска сетевых уязвимостей в NetRecon используется запатентованная технология UltraScan. Производимые NetRecon проверки тесно взаимосвязаны и результаты одной проверки используются для выполнения другой. Как и в случае реальных атак, в технологии UltraScan, информация об обнаруженных уязвимостях используется для выявления других связанных с ними уязвимостей. Например, если NetRecon удалось получить доступ к файлу,

содержащему пароли пользователей, и расшифровать несколько паролей, то эти пароли будут использованы для имитации атак на другие системы, входящие в состав сети.

NetRecon позволяет пользователю отслеживать путь поиска уязвимости, представляющий собой последовательность проверок, производимых NetRecon, которая привела к выявлению данной уязвимости. Путь поиска уязвимости позволяет проследить действия возможного нарушителя, осуществляющего атаку на сетевые ресурсы.

Используемая NetRecon база данных содержит описание известных уязвимостей и сценариев атак. Она регулярно пополняется новыми данными. Обновление этой базы данных производится через Web-узел компании Symantec автоматически, при помощи механизма LiveUpdate.

Сетевой сканер NESSUS. Сетевой сканер Nessus может рассматриваться в качестве достойной альтернативы коммерческим сканерам. Nessus является свободно распространяемым и постоянно обновляемым программным продуктом. Удобный графический интерфейс позволяет определять параметры сеанса сканирования, наблюдать за ходом сканирования, создавать и просматривать отчеты. По своим функциональным возможностям сканер защищенности Nessus находится в одном ряду, а по некоторым параметрам и превосходит такие широко известные коммерческие сканеры, как NetRecon компании Symantec, Internet Scanner компании ISS и CyberCop Scanner компании NAI.

Версии 0.99 серверной части сканера Nessus была сертифицирована в Гостехкомиссии России (Сертификат N 361 от 18 сентября 2000 г.).

Сценарии атак реализованы в NESSUS в качестве подключаемых модулей (plugins). Количество подключаемых модулей постоянно увеличивается, в настоящее время насчитывается более 700. Новые внешние модули,

эмулирующие атаки, можно инсталлировать, скопировав файлы, содержащие их исходные тексты, с web-сервера разработчиков www.nessus.org.

Nessus предоставляет очень широкие возможности по поиску уязвимостей корпоративных сетей и исследованию структуры сетевых сервисов. Помимо использования стандартных способов сканирования TCP и UDP портов, Nessus позволяет осуществлять поиск уязвимостей в реализациях протоколов управления сетью ICMP и SNMP. Кроме того, поддерживаются различные стелс-режимы сканирования, реализуемые популярным некоммерческим стелс-сканером nmap, который можно рассматривать в качестве одного из компонентов сканера Nessus. Другой популярный некоммерческий сканер queso используется в составе Nessus для определения типа и номера версии сканируемой ОС.

Высокая скорость сканирования достигается за счет использования при реализации сканера Nessus многопотоковой архитектуры программирования, позволяющей осуществлять одновременное параллельное сканирование сетевых хостов. Для сканирования каждого хоста сервером nessusd создается отдельный поток выполнения. Подробное описание используемых методов сканирования TCP/UDP портов можно найти в онлайновой документации на сканер nmap. Они включают в себя следующее:

- TCP connect scan
- TCP SYN scan
- TCP FIN scan
- TCP Xmas Tree scan
- TCP Null scan
- UDP scan

При реализации Nessus использована нетипичная для сетевых сканеров клиент/серверная архитектура. Взаимодействие между клиентом и сервером осуществляется по защищенному клиент-серверному протоколу, предусматривающему использование надежной схемы аутентификации и шифрование передаваемых данных. Сервер nessusd, работает только в среде UNIX и предназначен для выполнения сценариев сканирования. Механизмы собственной безопасности, реализованные в сервере nessusd позволяют осуществлять аутентификацию пользователей сканера, ограничивать полномочия пользователей по выполнению сканирования и регистрировать все действия пользователей в журнале регистрации событий на сервере.

Клиентская часть Nessus работает и в среде UNIX и в среде Windows и реализует графический интерфейс пользователя для управления сервером nessusd. Пользователь сканера, перед запуском сеанса сканирования, определяет параметры сканирования, указывая диапазон сканируемых IP-адресов и TCP/UDP портов, максимальное количество потоков сканирования (число одновременно сканируемых хостов), методы и сценарии сканирования (plugins), которые будут использоваться.

Все сценарии сканирования разделены на группы по типам реализуемых ими сетевых атак (Рисунок 8), обнаруживаемых уязвимостей, а также по видам тестируемых сетевых сервисов. Так, имеется специальная группа сценариев Backdoors для обнаружения троянских программ, Gain Shell Remotely - для реализации атак на получение пользовательских полномочий на удаленной UNIX системе, Firewalls – для тестирования МЭ, FTP – для тестирования FTP-серверов, Windows – для поиска уязвимостей Windows-систем и т.п.

Особую группу сценариев сканирования Denail of Service составляют атаки на отказ в обслуживании (DoS). Единственный способ убедиться в том, что сканируемая система подвержена той или иной DoS – это выполнить эту атаку и посмотреть на реакцию системы. Эта группа сценариев, однако, является

потенциально опасной, т.к. их запуск может привести к непредсказуемым последствиям для сканируемой сети, включая сбои в работе серверов и рабочих станций, потерю данных и «полный паралич» корпоративной сети. Поэтому большинство DoS в данной группе по умолчанию отключено.

Для написания сценариев атак служит специализированный C-подобный язык программирования высокого уровня NASL (Nessus Attack Scripting Language). Существует также интерфейс прикладного программирования (API) для разработки подключаемых модулей со сценариями атак на языке C, однако предпочтительным является все же использование NASL.

NASL является интерпретируемым языком программирования, что обеспечивает его независимость от платформы. Он предоставляет мощные средства для реализации любых сценариев сетевого взаимодействия, требующих формирования IP-пакетов произвольного вида.

Результаты работы сканера Nessus представлены на Рисунок 9. Данные об обнаруженных уязвимостях отсортированы по IP-адресам просканированных хостов. Найденные уязвимости проранжированы. Наиболее критичные (security holes) выделены красным цветом, менее критичные (security warning) – желтым. По каждой уязвимости приводится ее описание, оценка ассоциированного с ней риска (Risk Factor) и рекомендации по ее ликвидации (Solution).

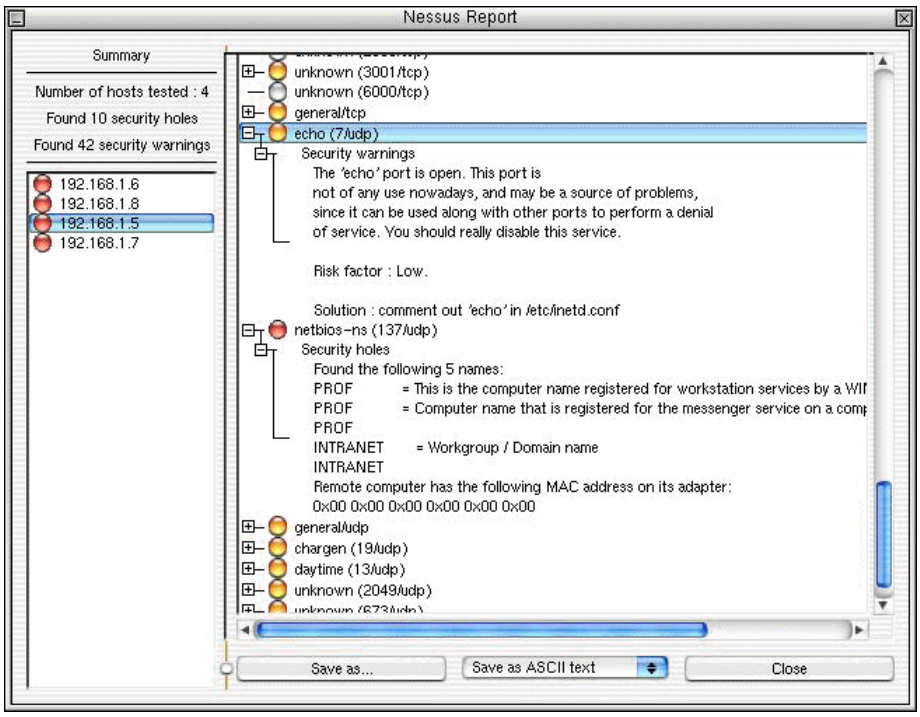


Рис. 2.12. Представление результатов сканирования в сканере Nessus

Средства контроля защищенности системного уровня. Обеспечение безопасности компьютерных систем, по существу, заключается в определении множества возможных угроз, оценке величины связанных с ними рисков, выборе адекватных контрмер, реализации этих контрмер процедурными и программно-техническими средствами и контроле их осуществления. Последний вопрос является, пожалуй, одним из наиболее сложных. Реализация программно-технических мер защиты требует произведения настроек большого количества параметров ОС, МЭ, СУБД, сетевых сервисов, прикладных программ и активного сетевого оборудования. Когда речь идет о защите отдельного сервера или рабочей станции, то задача хоть и является сложной, но ее решение вполне по силам опытному системному администратору. В этом случае для контроля значений параметров программ, связанных с безопасностью, используются специальные списки проверки. Когда же речь заходит о настройке десятков и сотен сетевых устройств, функционирующих на различных программно-аппаратных платформах, в соответствии с единой политикой безопасности, контроле параметров защиты и мониторинге безопасности в реальном масштабе времени, то без специальных средств

автоматизации уже не обойтись. Производители ОС предоставляют специальный инструментарий для контроля целостности и анализа защищенности ОС (утилита C2 Configuration в Windows NT Resource Kit, утилита ASET в ОС Solaris и т.п.). Имеется немало свободно распространяемых и широко используемых продуктов, предназначенных для решения подобных задач, таких как программа COPS для ОС UNIX. Однако эти средства, функционирующие на системном уровне, позволяют обеспечить только некоторый базовый уровень защищенности самой ОС. Для контроля приложений, сетевых сервисов, активного сетевого оборудования в распределенных системах, функционирующих в динамичной агрессивной среде необходимо использовать специализированный инструментарий, поддерживающий распределенные архитектуры, централизованное управление, различные программно-аппаратные платформы, различные виды приложений, использующий изощренные алгоритмы поиска и устранения уязвимостей, интегрированный с другими средствами защиты и удовлетворяющий многим другим требованиями, предъявляемым к современным продуктам этого класса.

2.3. Метод мониторинга безопасности при функционировании инфокоммуникационных систем

Формализация методов формирования и принятия решений при проектировании системы безопасности современных информационных систем (ИС) является весьма непростой задачей. Это, с одной стороны, объясняется сложностью и, как следствием, опасностью самих ИС, характеризуемых многоуровневыми архитектурами, распределенностью, использованием внешних сервисов и предоставлением во внешний мир своих, ограниченными временными рамками и т.д. С другой – сам процесс принятия решений, учитывающий целый спектр противоречивых факторов, включающий вопросы законодательного, административного, процедурного, программно-технического аспектов не менее сложен, чем сам объект защиты.

Увеличение объема информации, которую необходимо проанализировать экспертам, усложнение решаемых задач, необходимость учета большого числа взаимосвязанных факторов требуют использования вычислительной техники в процессе принятия решений. В связи с этим появился новый класс систем – систем поддержки принятия решений (СППР), основанных на формализации методов получения объективных и субъективных оценок, алгоритмизации рассуждений, анализа ситуаций, выработки вариантов решений. Одной из задач СППР при организации защиты является мониторинг параметров функционирования объекта защиты, на основании анализа данных которого решается вопрос о необходимости проектирования системы безопасности обследуемого объекта.

В статье определены области функционирования объекта защиты, параметры которых должны быть подвержены процедуре мониторинга; сформулированы задачи, стоящие перед подсистемой мониторинга, описаны компьютерные процедуры и алгоритмы анализа, использующие аппарат субъективных оценок.

Описание объекта защиты. В [1] подчеркивалось, что основными защищаемыми активами компании являются бизнес-процессы, совокупность которых ассоциируются с корпоративной информационной системой (КИС).

При организации защиты активов КИС может быть две ситуации:

1. информационная система – в стадии разработки и одновременно с ней происходит проектирование защиты как межкатегорийного сервиса [2] ИС. Тогда речь следует вести не о мониторинге, а скорее, о прогнозировании параметров функционирования бизнес-процессов, включая и параметры безопасности.

2. информационная система – в стадии эксплуатации и стоит задача спроектировать для ее бизнес-процессов систему безопасности. Именно эта ситуация и рассматривается в данной работе.

Понятие бизнес-процесса включает: а). некоторую семантику, реализуемую бизнес-логикой (виды деятельности и их взаимосвязь), б). среду функционирования, которую можно представить моделью OSE\RM (Open system environment\ reference model) группы POSIX (Portable Operating System Interface for Unix), представляющую собой трехмерную логическую (справочную, эталонную, референсную) структуризацию функциональности информационной системы и описанную в [2,3] (на рис.2.13. представлен пример некоторых реализаций «клеток» модели). Уровни описания в данной модели следующие:

- компоненты служб и сервисов промежуточного слоя (MW);
- компоненты операционных систем или операционного слоя (OW);
- аппаратный слой (HW).

Функциональные группы компонентов в данной модели составляют:

- компоненты, обеспечивающие интерфейс с пользователем (User - "U");
- компоненты, обеспечивающие всех необходимых процессов в системе (System - "S");
- компоненты, обеспечивающие организацию, представление, доступ и хранение данных (Information - "I");
- компоненты телекоммуникационной среды, обеспечивающие взаимосвязь информационных систем (Communication - "C"), данный уровень представляет собой модель взаимосвязи открытых систем (OSI/RM–Open System Interconnection/Reference

Model).

Компоненты среды определяют параметры функционирования бизнес-процесса, а с точки зрения информационной безопасности она является носителем различного рода уязвимостей, которые используются нарушителем для проникновения в КИС.

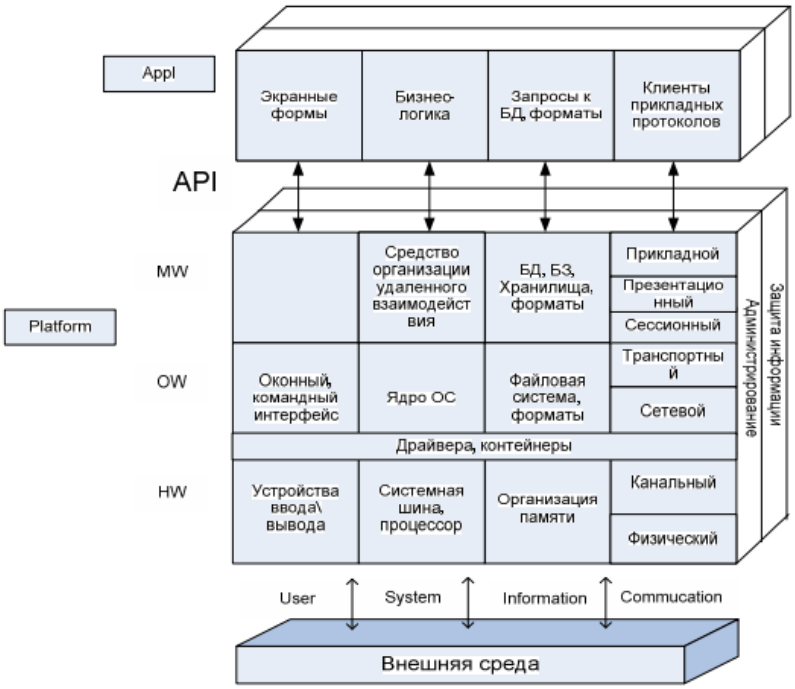


Рис.2.13. Модель OSE\RM

Первый этап, с которого следует начать проектирование защиты бизнес-процессов, это мониторинг и анализ состояния среды бизнес-процессов. Задачами подсистемы мониторинга СППР при проектировании системы безопасности являются: систематическое накопление данных о функционировании бизнес-процессов, обработка и анализ этих данных, представление результатов анализа в виде, удобном для ЛПР.

Анализ осуществляется с целью определения необходимости организации дополнительной защиты тому или иному бизнес-процессу. Проводить его будем по следующим направлениям:

1. Идентификация и оценка ценности информационных ресурсов КИС.
2. Загрузка вычислительных ресурсов бизнес-процесса.
3. Опасность среды бизнес-процесса с точки зрения проникновения нарушителя, ее уязвимость.
4. Защищенность, которая обеспечивается встроенными в среду средствами защиты.

Оценка ценности информационных ресурсов, обрабатываемых бизнес-процессом. Прежде всего следует заметить, что ценность информационных ресурсов и ущерб от компрометации этих ресурсов – это две стороны одной медали. Например, если клиентская БД страховой компании попала в руки к конкурентам, компания понесет ущерб в объеме недополученных страховых сборов. Поэтому оценка ценности ресурсов одновременно влечет и оценку ущерба от компрометации этих ресурсов.

К информационным ресурсам, в первую очередь, относится так называемый интеллектуальный капитал (ИК) организации, включая нематериальные активы. В [11] определен следующий состав ИК:

1. Рыночный, т.е. активы предприятия, связанные с рыночными операциями, обеспечивающими конкурентные преимущества (данные по клиентам, поставщикам, партнеров по бизнесу, репутация компании и т.д.).

2. Структурный, который включает объекты интеллектуальной собственности (данные по патентам, авторским правам, производственным, инновационным, управленческим секретам, и т.д.), и активы, формирующие рабочую среду фирмы (корпоративные, технологические, производственные стандарты, бизнес-правила, учетные политики и т.д.)

3. Человеческий капитал, воплощающий коллективные и индивидуальные знания компании, но контекст безопасности – это законодательная охрана персональных данных.

Перечисленные интеллектуальные активы в виде различных по семантике БД, хранилищ, отдельных файлов привязаны как внешние сущности к бизнес-процессам; при моделировании последних подсистема мониторинга ведет учет этих сущностей. Таким образом осуществляется структуризация ИК, в результате чего все информационные ресурсы КИС ставятся в соответствие «клеткам» платформенной компоненты, а именно, столбцу Information того или иного бизнес-процесса.

Кроме того, при оценке ущерба следует принять во внимание и тот факт, что он может произойти и в случае, если какая-либо функция бизнес-

процесса перестает работать. Поэтому при оценке ценности\ущерба к информационным ресурсам отнесем не только активы ИК, но и исполняемые коды ПО.

Ценность\ущерб может выражаться как в денежном, так и в неденежном исчислении (например, санкции, которые понесет руководитель за нарушение закона о защите персональных данных). Поэтому есть смысл перейти к обобщенному показателю «приоритет ресурса» Pr, который будет измеряться лингвистической или балльной шкалой: «высокий-4», «средний-3», «низкий-2», «очень низкий-1» (через дефис здесь и далее в лингвистических шкалах приведены балльные оценки).

Оценочные критерии при определении значений приоритета Pr активов ИК могут

быть следующие:

К1. Нормативные акты, которые регламентируют актив: «закон РФ-4», «ГОСТ-3», «РД-2», «внутренние документы-1»; (этот критерий имеет свою лингвистическую шкалу, но она волне согласуется с общей).

К2. Конкурентные преимущества.

К3. Объем недополученного дохода.

К4. Степень личной ответственности ЛПР.

К5. Степень юридической ответственности.

К6. Стоимость восстановления кодов.

К7. Стоимость восстановления аппаратных средств.

К8. Потери от компрометации брэнда.

К9. Стоимость восстановления данных и т.д.

Состав списков критериев определяется семантикой функций бизнес-процессов и может быть предварительно сгенерирован в подсистеме моделирования бизнес-процессов.

Далее по каждому активу «клетки» подсистема мониторинга предлагает предварительные списки каждому эксперту, которые они могут утвердить или модифицировать. После этого СППР проводит процедуру

согласования списков экспертов. Алгоритмы согласования хорошо известны, в систему могут быть заложены несколько с тем, чтобы ЛПР мог выбрать процедуру согласования. На рис. 2.14. приведена блок-схема процедуры согласования, проводимой СППР, которая включает блоки автоматического и ручного согласования [4].

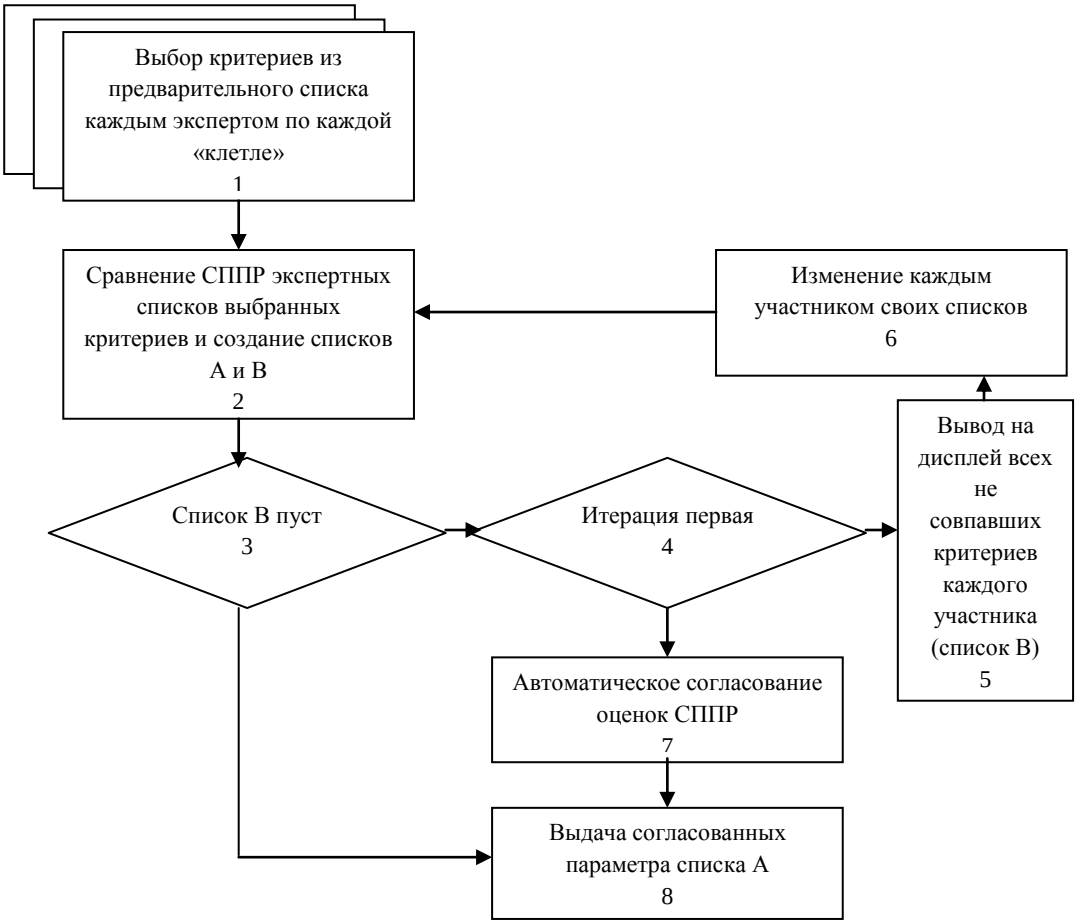


Рис. 2.14. Блок-схема процедуры согласования

Комментарии к блокам, требующим пояснения

Блок 2 проводит сравнение экспертных списков и создает два списка параметров: список А, в который вошли критерии, выбранные всеми экспертами, и список В, содержащий все остальные критерии. Список В подлежит дальнейшему согласованию.

Блок 4 проверяет номер итерации. Если итерация первая – переход к блоку 5, если нет – к блоку 7. Вообще итераций может быть сколь угодно много, но опыт показывает, что на последующих итерациях скорость

сходимости падает или сближение оценок вообще прекращается. Поэтому после первой (или первых) итераций лучше перейти к какому-либо методу их автоматического согласования

Блок 7. Автоматическое согласование, проводимое СППР с использованием процедур голосования, тогда в списке остаются те критерии, которые прошли ту или иную процедуру голосования. В настоящее время в литературе описано достаточно много процедур голосования, с которыми можно ознакомиться, например, в [5].

Важно отметить, что от выбора процедуры может зависеть ее результат, поэтому выбор процедуры может вызвать дискуссию, но процедура может быть определена и руководителем.

Пусть после первой итерации ЛПР решил провести голосование по правилу абсолютного большинства, т.е. считать согласованными те критерии, за которые проголосовали больше половины экспертов. СППР сравнивает перечень параметров в списке В и определяет число экспертов, давших одинаковые оценки. Оказалось, что у большинства экспертов оценки совпадают. Система записывает эти оценки в список А, ликвидируя список В.

Процедура согласования списка критериев по «клеткам» закончена.

В табл. 2.1 приведен пример согласованных оценок приоритета ресурсов «клеток» S_i-го бизнес-процесса по списку критериев К1, К2, К3.

Таблица 2.1.

Идентификатор «клетки» бизнес-процесса S_i	Критерий			$Pr(K_p)$
	Нормативные акты	Конкурентные преимущества	Оббьем недополученного дохода	
$К_1$	РД – 2	Очень низкий – 1	Средний - 3	1.92
. . .	. . .	. . .	. . .	. . .
$К_p$	ГОСТ - 3	Средний - 3	Высокий – 4	3.09
Средние значения	$Pr^{R1}(S_i)$	$Pr^{R2}(S_i)$	$Pr^{R3}(S_i)$	$Pr(S_i)$

Таблица 2.1. Пример согласованных оценок приоритета ресурсов.

Здесь $Pr^{K1}(S_i)$, $Pr^{K2}(S_i)$, $Pr^{K3}(S_i)$, - приоритеты бизнес-процесса по критериям К1, К2 и К3 соответственно, кот орые считаются как средние по столбцу.

Последний столбец таблицы содержит приоритеты «клеток», которые представляют собой линейные функции

$$Pr\ (K_p) = \sum_S a_{ps} x_{ps} \qquad (1)$$

где a_{ps} – вес критерия, x_{ps} – значения критерия, а также совокупную оценку приоритета всего бизнес-процесса $Pr(Si) = \frac{1}{P}\sum_{P=1}^{P} \Pr(K_p)$ которая потребуется в дальнейшем при ранжировании целей безопасности.

Далее следует определить значимость критериев, их вес a_{ps}. Для этого можно использовать известные методы [4] или заполнить каждому эксперту таблицу рангов (значимости). Ранг критерия определяет, какова по мнению экспертов, его важность (табл.2).

В таблицах 2.1, 2.2 все значения критериев иллюстративного примера представлены в лингвистической форме. Для дальнейшего анализа потребуются балльная форма оценок, обычно такой перевод подсистема мониторинга делает автоматически (в скобках даны их балльные соответствия).

Таблица 2.2

Идентификатор «клетки» бизнес-процесса S_i	Важность критерий		
	Нормативные акты	Конкурентные преимущества	Обьем недополученного дохода
$К_1$	Высокая - 3	Низкая – 1	Средняя – 2
. . .	. . .	. . .	. . .
$К_р$	Низкая - 1	Средняя - 2	Очень высокая – 4

Таблицы типа 2.1, 2.2 определяющие балльные или лингвистические оценки критериев и их веса, составляются экспертами заранее и согласовываются в подсистеме предпроектного проектирования СППР.

После того, как каждый эксперт проставил ранги в таблицах 2 для каждой «клетки» СППР определяет сумму рангов, набранным каждым критерием:

$r_{ps}=\sum_{j=1}^{J} r_{js} n_s$, где r_{js}– ранг s-го критерия, определенный j-м экспертом для *p*-ой «клетки», n_s – число экспертов, давших данную оценку критерию, а также вес критерия, т.е нормированную сумму рангов $a_{ps}=\frac{r_{ps}}{\sum_s r_{ps}}$

В итоге получим табл. 2.3, последний столбец которой содержит значения весов a_{ps} из

Таблца. 2.3.

Идентификатор «клетки» бизнес-процесса S_i	Оценка важности критерия												Сумма рангов критериев r_{pj}			Нормированный вес a_{pj}		
	Нормативные акты				Конкурентные преимущества				Объем недополученного дохода									
	n=4	n=3	n=2	n=1	n=5	n=2	n=2	n=1	n=4	n=3	n=2	n=1	K_1	K_2	K_3	K_1	K_2	K_3
K_1	3	2	4	1	4	2	3	1	2	4	1	3	27	31	25	0.33	0.37	0.3
…….	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
K_P	2	4	3	2	3	4	1	2	1	1	2	3	28	27	14	0.41	0.39	0.2

Оценка загрузки вычислительных ресурсов бизнес-процесса. Мониторинг загрузки вычислительных ресурсов среды бизнес-процесса необходимо осуществлять с двумя целями. Первая – фиксация эталонных значений, т.е. определение штатного режима функционирования параметров среды, осуществляется стандартными программными средствами. В дальнейшем это позволит СППР оценивать отклонения текущих значений от эталонных и определять наличие инцидентов безопасности.

Параметры, по которым отслеживается загрузка вычислительных ресурсов, структурируются в соответствии с базовой плоскостью платформенной части модели OSE\RM. Оценку этих параметров целесообразно производить по следующим критериям:

1. Степень загрузки того или иного оборудования (производится по аппаратному слою референсной модели – рис.1).

2. Степень разбалансировки загрузки сетевого оборудования (столбец Communication) и оборудования столбцов User, System, Information.

3. Отклонение от штатных значений и т.д.

Измеряются критерии по лингвистической однородной шкале «отсутствует-0», «низкая-1», «средняя-2», «высокая-3», «критическая-4».

Вторая цель – утилитарная. Системный администратор, имея списки подключенных модемов, сканирующих программ, открытых портов, сетевых сервисов и т.д., может провести анализ на защищенность\незащищенность, легитимность\нелигитимность, нужность\ненужность соответствующих объектов.

Оценка параметров уязвимости среды бизнес-процесса. Среда, которая представляется «клетками» платформенной компоненты OSE\RM, подвержена влиянию ряда объективных факторов, декларируемых стандартом ИСО\МЭК 15408 [6]:

- угрозы информационной безопасности со стороны среды бизнес-процесса $Y(S_i)$, где $i=1 \div I$, I – количество автоматизированных бизнес-процессов предприятия, характеризующиеся вероятностью возникновения и вероятностью реализации;
- уязвимости среды бизнес-процесса или системы контрмер $\tilde{X}$ ($\tilde{x}_1, \tilde{x}_2, \ldots \tilde{x}_n$), влияющие на вероятность реализации угрозы;
- нарушитель, определяющий вероятность возникновения угрозы;
- риск – фактор, отражающий возможный ущерб в результате реализации угрозы.

Пусть $P(A(\tilde{x}_i))$–вероятность реализации той или иной угрозы, здесь $A(\tilde{x}_i)$-событие, интерпретируемое как использование нарушителем уязвимости $\tilde{x}_i$;

$U(S_i)$–величина возможного ущерба при нарушении штатного функционирования бизнес-процесса S_i.

Тогда количественный уровень риска определяется как функция

$R(S_i) = f\,(P(A(\tilde{x}_i)),U(S_i)))$.

При этом вероятностные оценки будем рассматривать в рамках субъективного подхода, который рассматривает вероятность как субъективную меру убежденности наблюдателя, соответствующую его знаниям и опыту, в истинности или ложности предложенного ему утверждения [7]. Тогда оценку меры риска *Risk(Si)*, присущего бизнес-процессу, можно определить как произведение оценки угрозы $Y(S_i)$ на оценку ценности ущерба $Pr(S_i)$

$$Risk(S_i)= Y(S_i) * Pr(S_i).$$

Итак, среда бизнес-процесса несет угрозы его безопасности, т.к. является носителем уязвимостей $\tilde{X}$, т.е. тех огрехов в ПО или защите, которые могут быть использованы нарушителем. Рассматриваются два типа уязвимостей: технологические – это «дыры» в программном коде платформенной или прикладной компонент, появляющиеся на стадии разработки ПО, или самих средств защиты, и эксплуатационные.

Уязвимости являются основной предпосылкой нападения нарушителя и существуют объективно на момент планирования защиты. Стало быть, анализирующий блок подсистемы мониторинга должен оценить ту долю риска, который присущ среде вследствие имеющихся уязвимостей. Механизм оценки может быть следующий.

1. С помощью определенного ПО (сканеры уязвимостей) для конкретной реализации среды бизнес-процесса на стадии предпроектного проектирования СППР выявляются перечни уязвимостей $\tilde{X}\,(\tilde{x}_1, \tilde{x}_2, \ldots \tilde{x}_n)$и ставятся в соответствие «клеткам».

2. Любую уязвимость $\tilde{x}_i$ можно характеризовать двумя действиями: сначала идентифицировать уязвимость, а затем ее использовать. $\forall \tilde{x}_i$ с точки зрения этих действий характеризуется следующими параметрами:

a. временем, которое необходимо для совершения этих действий,

b. необходимой квалификации,

c. уровнем знаний о среде,

d. характером и продолжительностью доступа к среде,

e. необходимыми аппаратно-программными ресурсами.

Для каждого критерия в СППР имеются согласованные экспертами оценочные балльные шкалы, разработанные на основе [8] (в табл. 2.4 приведен пример шкалы по критерию а), оценочные шкалы остальных критериев можно посмотреть там же).

Таблица 2.4.

Время	Идентификация уязвимости	Использование уязвимости
< 0,5 часа	0	0
< суток	2	3
< месяца	3	5
>месяца	5	8

Далее для $\forall \tilde{x}_i$ СППР получает общую оценку (рейтинг уязвимости) по алгоритму, описанному в [8], который использует используют аддитивную функцию, т.е. выбранные значения по обоим действиям по всем таблицам суммируются. Если уязвимость можно идентифицировать\использовать несколькими способами, для каждого из них вычисляется рейтинг и из полученных значений выбирается минимальное, т.е. уязвимость характеризуется самым простым методом успешного нападения. По этому же правилу по всем $.\tilde{x}_i$ «клетки» вычисляется общий рейтинг $R^{клетки}$,т.е. $R^{клетки}$= $\min(R^{\tilde{x}_1}, R^{\tilde{x}_2}, \ldots, R^{\tilde{x}_i})$, где $R^{\tilde{x}_i}$ -рейтинг уязвимостей, принадлежащих данной «клетке». Оценочная шкала рейтинга уязвимостей приведена в табл. 2.5.

Таблица 2.5

Диапазон $R^{клетки}$	Рейтинг уязвимости
< 10	Низкий – 1
10 – 17	Умеренный – 2
18 – 24	Высокий – 3
> 24	Нереально высокий - 4

3. По тому же принципу вычисляется потенциал нарушителя *NP*. В [8] этот потенциал с учетом правила максимума $NP = max(NP^1, NP^2, \ldots, NP^n)$(из нескольких сценариев нападения выбирается худший вариант, с наибольшим потенциалом) определяется оценками табл.2.6.

Таблица 2.6

Диапазон *потенциала*	Потенциал нарушителя
< 10	Низкий – 1
10 – 17	Умеренный – 2
18 – 24	Высокий – 3
> 24	Нереально высокий - 4

Оценка защищенности встроенными средствами. Защита среды бизнес-процессов от несанкционированного вмешательства в процессы их функционирования обеспечивается специальными механизмами. В литературе [6,8] описываются следующие защитные механизмы (*Mx*):

1. Идентификация и аутентификация пользователя;

2. Разграничение доступа пользователей к ресурсам бизнес-процесса;

3. Мониторинг и аудит событий, происходящих в системе;

4. Криптографическая поддержка (шифрование) хранимых и передаваемых данных;

5. Контроль целостности и аутентичности (подлинности и авторства) хранимых и

передаваемых данных;

6. Экранирование компьютерной сети, т.е. защита ее периметра;

7. Анализ защищенности, т.е. выявление и анализ уязвимостей среды бизнес-процесса;

8. Обеспечение отказоустойчивости (живучести) среды бизнес-процессов, т.е. способности сохранять требуемую эффективность, несмотря на отказ отдельных элементов;

9. Обеспечение обслуживаемости, т.е. способности к быстрому и безопасному восстановлению;

10. Туннелирование, т.е. «упаковка» передаваемого пакета данных в новый «конверт»;

11. Уничтожение остаточных на носителях данных;

12. Выявление и нейтрализация вирусов;

13. Обнаружение компьютерных атак;

14. Управление, обеспечивающее согласованное функционирование средств защиты.

Каждый механизм реализуется методами, алгоритмы которых и обеспечивают тот или иной уровень защиты. Традиционно уровень защиты принято определять стойкостью механизмов. Под стойкостью понимается характеристика, отражающая минимальные усилия нарушителя, необходимые для нарушения безопасности, обеспечивающейся данным механизмом [9]. Параметр оценивается шкалой «Стойкость»: «базовая-1», «средняя-2», «высокая-3».

В свою очередь, совокупности механизмов реализуются в виде тех или иных средств защиты, которые делятся на два класса:

1.Механизмы, встроенные (штатные) в покупаемое программное обеспечение. Многие программные и аппаратные средства, которые реализуют «клетки» референсной модели, имеют встроенные защитные механизмы, реализованные программно и установленные разработчиками этих средств: операционные системы, СУБД, различные приложения реализуют механизмы идентификации и аутентификации, обладают свойствами межсетевых экранов, средствами шифрования и т.д. Таким

образом, на момент проектирования системы безопасности среда бизнес-процесса в той или иной мере защищена. Стало быть, одной из задач мониторинга является определение уровня защиты, которую могут обеспечить штатные средства.

2.Наложенные, т.е. реализованные как самостоятельные программные или программно-аппаратные комплексы и устанавливаемые дополнительно.

На стадии предпроектного проектирования подсистема мониторинга в интерактивном режиме опрашивает экспертов и сопоставляет каждой «клетке» реализованные в ней штатные механизмы. СППР заполняет таблицу стойкости типа табл.2.7.

Таблица 2.7

Идентификатор «клетки» бизнес-процесса S_i	Стойкость механизмов $S(Mx_k)$			$S(Mx_p)$
	Mx_1	. . .	$Mx_к$	
1	2	. . .	k	k + 1
$К_1$	Высокая – 3	. . .	Базовая – 1	Умеренная
. . .	. . .	. . .	. . .	. . .
$К_р$	Средняя – 2		Механизм отсутствует	Средняя
Средние значения $S(Mx_k)$	Средняя - 2		Базовая - 1	$S(Mx)$

Здесь $S(Mx_k)$ – стойкость k-го защитного механизма.

$\bar{S}(Mx_k)$ - средняя стойкость k-го механизма по бизнес-процессу, вычисляется по недостатку по шкале «Стойкость» $\bar{S}(M_{xk})=\left\lfloor \frac{1}{p}\sum_p x_p \right\rfloor$, $x_р$-оценки механизмов по столбцу 2 ÷ k.

$S(Mx_p)$–совокупная стойкость механизмов, соответствующих p-ой «клетке» – представляет собой суждения экспертов о величине синергетического защитного эффекта от влияния механизмов друг на друга. Например, туннелирование по протоколу IPv6 над стандартным TCP/IP дает достаточно низкую безопасность по конфиденциальности при передаче данных, но вкупе с механизмом шифрования уровень конфиденциальности резко повышается, а, если на концах канала передачи установить межсетевой

экран, получим одно из самых надежных средств защиты – виртуальную частную сеть VPN.

Оценка $S(Mx_p)$ производится экспертами следующим образом:

1. каждый эксперт на основании столбцов 2 ÷ k выставляет совокупную оценку. Для этого вводится шкала «Совокупная стойкость»: «низкая-1», «умеренная-2», «высокая-3», «очень высокая-4», т.к. шкала «Стойкость», предлагаемая стандартами [6,9], не обеспечивают однородность оценочных шкал.

2. согласование совокупных оценок по вышеприведенному алгоритму. В табл.7 приведен пример согласованных оценок.

$\bar{S}(Mx)$– средняя совокупная стойкость механизмов бизнес-процесса, вычисляется по недостатку как среднее по столбцу $\bar{S}(Mx_k) = \left\lfloor \frac{1}{p}\sum_p x_p \right\rfloor$, x_p- совокупные оценки механизмов по столбцу k+1.

Анализ параметров мониторинга. Анализ взаимосвязей этих параметров позволяет решить вопрос о достаточности \не достаточности штатных механизмов.

Итак, в результате мониторинга получим распределение параметров по референсной модели, представленное на рисунке 2.15, где каждая «клетка» оценивается рейтингом уязвимостей $R^{клетки}$, потенциалом нарушителя NP, который может воспользоваться уязвимостями клетки $\tilde{X}^{клетки}$, стойкостью $S(Mx_p)$ защитных средств и приоритетом ресурсов $Pr(K_p)$, сопоставленных данной «клетке».

MW		$R^{клетки}$ $S(Mx_1)$ NP $Pr(K_1)$	$R^{клетки}$ $S(Mx_1)$ NP $Pr(K_1)$	$R^{клетки}$ $S(Mx_1)$ NP $Pr(K_1)$
SW	$R^{клетки}$ $S(Mx_1)$ NP $Pr(K_1)$	$R^{клетки}$ $S(Mx_1)$ NP $Pr(K_1)$	$R^{клетки}$ $S(Mx_1)$ NP $Pr(K_1)$	$R^{клетки}$ $S(Mx_1)$ NP $Pr(K_1)$
HW	$R^{клетки}$ $S(Mx_1)$ NP	$R^{клетки}$ $S(Mx_1)$ NP	$R^{клетки}$ $S(Mx_1)$ NP	$R^{клетки}$ $S(Mx_1)$ NP

$Pr(K_1)$	$Pr(K_1)$	$Pr(K_1)$	$Pr(K_1)$
User	System	Information	Communication

Рис.2.15. Матрица параметров мониторинга в соответствии с моделью OSE\RM

Соотношение параметров определяется по следующим правилам:

1. СППР рассматривает пару рейтинг «клетки» $R^{клетки}$ – потенциал нарушителя *NP*. Первое решающее правило гласит: нарушитель может совершить успешное нападение на ресурсы «клетки», если его потенциал не меньше рейтинга уязвимости, т.е., если рейтинг уязвимости имеет, например, оценку «умеренный», то для успешного нападения потенциал нарушителя должен быть «высокий» (см. рис.).

Таким образом, условие успешного нападения заключается в том, что существует $NP = \max (NP^j)$ такое, что $R^{клетки} < NP$, где j – типы нарушителя.

2.С другой стороны, нападение нейтрализует защитный механизм, обладающий определенной стойкостью, т.е. необходимо сравнить пару: потенциал нарушителя *NP* – стойкость механизмов $S(Mx_p)$. Сравнение будем проводить следующим образом: если $S(Mx_p) \geq NP$, то нападение нарушителя будет отражено защитным механизмом и

уязвимости «клетки» не «сыграют».

Рис. 2.16 демонстрирует схему сравнения параметров $R^{клетки}$, *NP* и $S(Mx_p)$ в нечетких шкалах по правилам 1 и 2.

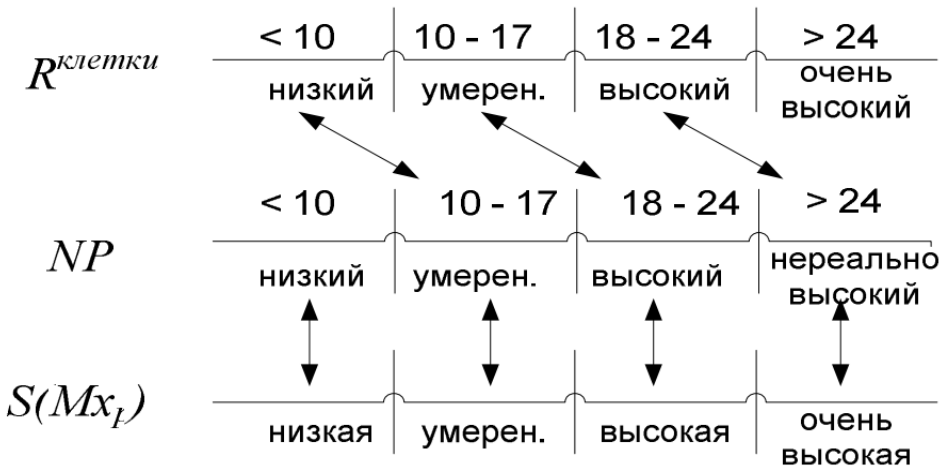


Рис. 2.16. Схема сравнения параметров по правилам 1, 2

3. В результате проверки правил 1 и 2 для параметров NP, $S(Mx_p)$, $R^{клетки}$ подсистема мониторинга делает вывод о степени реализации угрозы Y_p для той или иной «клетки». При этом возможны следующие девять ситуаций:

А). Ситуация, когда угроза осуществима: потенциал нарушителя превосходит рейтинг уязвимости, а стойкость защитных механизмов недостаточна.

Б). Ситуация, когда угроза почти осуществима: рейтинг уязвимости равен потенциалу, а стойкость механизмов превосходит ниже потенциала нарушителя.

В). Ситуация, когда угроза, скорее всего, осуществима, т.к. в силу приближенности оценок правило 2 может не сработать.

Г). Очень возможно, что угроза реализуется, т.к. потенциал выше рейтинга уязвимостей, хотя стойкость выше потенциала.

Д). Пограничная ситуация, когда потенциал нарушителя, рейтинг уязвимостей и стойкости механизмов соответствует друг другу, но, опять же, в силу приближенности и субъективности суждений ситуация требует пристального внимания со стороны ЛПР.

Е). Правило 1 не включает ситуацию равенства рейтинга и потенциала, но субъективность оценок требует, на наш взгляд, учета таких ситуаций. За счет стойкости, превосходящей потенциал, угроза может остаться нереализованной.

Ж). Ситуация, когда угрозы, скорее всего, нет, т.к. рейтинг выше потенциала, но недостаточная стойкость влечет некоторую неуверенность в благоприятном исходе.

З). Угрозы почти нет, т.к. рейтинг выше потенциала, а стойкость ему соответствует.

И). Ситуация, когда угроза точно не может быть реализована, т.к. оба правила дают положительные исходы.

Рис.2.16 демонстрирует графическое представление различные соотношения анализируемых параметров в соответствии с исходами правил 1, 2.

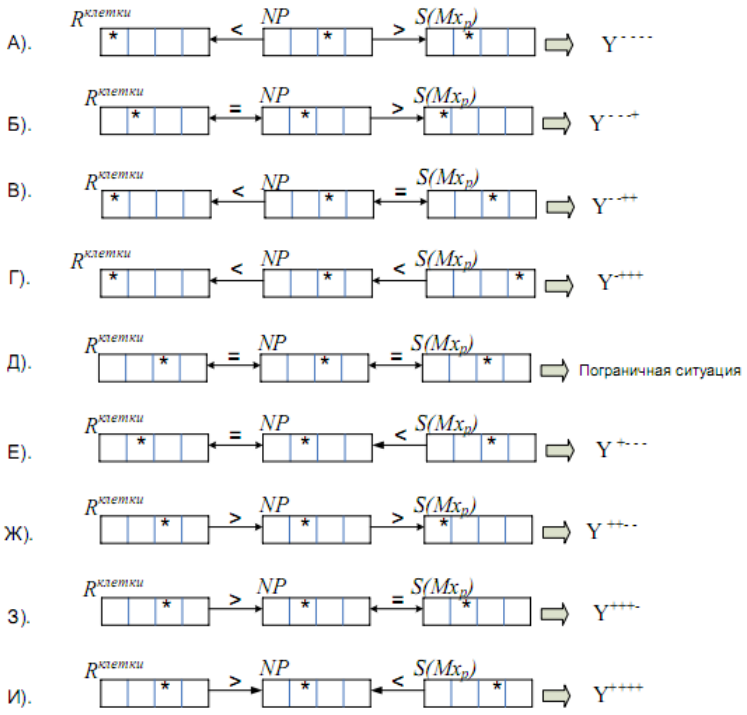


Рис. 2.17. Возможные ситуации при реализации угроз

Эти ситуации, отражающие степень реализации угрозы при наличии только штатных средств защиты, можно интерпретировать шкалой, представленной в табл.2.7.

Таблица 2.7

Идентификатор «клетки» бизнес-процесса S_i	Стойкость механизмов $S(Mx_k)$			$S(Mx_p)$
	Mx_1	. . .	Mx_K	
1	2	. . .	k	k +1
K_1	Высокая -3	. . .	Базовая -1	умеренная
. . .	. . .	. . .	. . .	. . .
K_P	Средняя -2		Механизм отсутствует	средняя
Средняя стойкость $\overline{S}(Mx_k)$	Средняя-2		Базовая -1	$\overline{S}(Mx)$

4. Вообще говоря, на основании выводов, представленных подсистемой мониторинга в соответствии с проведенным анализом, СППР может принять решение о необходимости привлечения наложенных средств защиты. Но, в дополнение к полученным оценкам, она может осуществить и анализ того, какие риски ожидают компанию, если угроза реализуется с

уверенностью Y_p. Риск – это категория, зависящая не только от степени реализации угрозы , но и от объема ущерба.

Тогда, на основании оценок ущерба и угроз подсистема мониторинга реализует алгоритм расчета оценки риска среды для p-х «клеток»

$Risk = \lfloor \Pr(K_p) \rfloor * Y_p$

где $Pr(K_p)$ – оценка ущерба, Y_p – оценка угрозы, $p=1,\ldots,P$.

Вычисленное значение $Risk_p$ отображается на шкалу «Риск клетки», которая формируется из следующих соображений. Формула (2) может дать 20 возможных произведений: 0, 1, 2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 24, 28, которые СППР автоматически может разнести по, например, 5-и балльной шкале, отнеся 0, 1, 2, 3 к уровню риска «очень низкий»; 4, 5, 6, 7 – к уровню «низкий»; 8, 9, 10, 12 – к «средний»; 14, 15, 16, 18 – к «выше среднего»; 20, 21, 24, 28 – к «высокий». Если такое разнесение экспертов не устроит, возможна процедура ручного формирования шкалы риска и разнесения по ней возможных значений $Risk_p$.

Совокупный по бизнес-процессу риск *Risk* подсистема мониторинга может определять двумя способами (хотя могут быть заложены и другие алгоритмы):

1.Как среднее значение по «клеткам» $Risk = \frac{1}{P}\sum_p Risk_p$

2.Как мультипликативная функция с учетом важности риска для «клетки» $Risk = \prod_p a_p Risk_p$. При этом СППР производит процедуру назначения и согласования весов «клеток» a_p с точки зрения риска по алгоритмам, описанным ранее.

Стратегии, связанные с управлением рисками, из которых ЛПР производит выбор могут быть различные, но существуют четыре стандартные:

Стратегия 1. Пусть $Risk^*$ - некоторый порог риска, приемлемого для компании с точки зрения ЛПР. Тогда, если $Risk < Risk^*$, то по данной клетке

компания готова нести потери в случае атаки злоумышленника, но систему безопасности из дополнительных средств проектировать не нужно.

Стратегия 2. Ликвидация риска, т.е сведение его до нулевого уровня.

Стратегия 3. Уменьшение риска до приемлемого уровня.

Стратегия 4. Переадресация риска – означает, что компания решает застраховать риски, связанные с информационными атаками и дополнительные средства защиты.

Стратегии 2 и 3 работают при условии $Risk \geq Risk^*$. Это означает, что при неприемлемом риске в дополнение к защитным штатным средствам необходимы наложенные, т.е. нужно проектировать комплексную систему защиты (КСЗ) из наложенных и штатных средств, а стало быть, необходимо реализовывать процедуру определения целевых векторов безопасности $KS_h^{цель}(K(T^*),C(T^*)D(T^*)$ где $K(T^*),C(T^*),D(T^*)$–уровни конфиденциальности, целостности, доступности соответственно, которые должна обеспечивать КСЗ для ресурсов, обрабатываемых бизнес-процессом. Состав вектора безопасности продиктован тем, что информационная безопасность обеспечивается именно перечисленными основными свойствами данных в информационных системах.

Выводы по второй главе

1. Рассмотренная формальная модель защищенной компьютерной сети показывает, что интегрированная система безопасности должна контролировать четыре уровня сетевого взаимодействия.
2. Анализ существующих аппаратно-программных средств мониторинга безопасности показал, что основными компонентами непрерывного контроля являются сетевые сканеры, которые позволяют обнаруживать уязвимости до их применения.
3. Исследование предложенного метода мониторинга безопасности при функционировании инфокоммуникационной системы показало, что при анализе параметров мониторинга необходимо учитывать характеристики, такие как загрузка вычислительных ресурсов, параметры уязвимостей и защищенности.

ГЛАВА 3. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ СИСТЕМЫ МОНИТОРИНГА БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

3.1 Применение proxy-серверов для организации системы мониторинга безопасности на примере использующих Internet –ресурсов.

В качестве разграничения доступа к глобальной компьютерной сети Internet используют proxy-сервер.

Программы браузеры в локальной сети сконфигурированы так, чтобы посылать все запросы proxy-серверу, вместо сервера в Internet, к которому они хотят обратиться. Proxy-сервер, в свою очередь, передает запрос соответствующему серверу в Internet, используя собственный IP-адрес как адрес источника запроса, принимает ответ от сервера и пересылает его клиенту, который изначально делал запрос.

Поскольку в Internet виден только адрес proxy-сервера, у внешних пользователей нет возможности получить доступ к пользовательским системам в этой локальной сети. Кроме того, proxy-сервер анализирует каждый пакет, пришедший из Internet, и только пакеты, которые являются ответом на определенный запрос, пересылаются дальше. Также proxy-сервера может самостоятельно исследовать данные на предмет наличия в них опасного кода или подозрительного содержания. Proxy-сервер имеет уникальные возможности регулирования трафика пользователя с большой точностью. Типичный proxy-сервер Web, например, дает возможность сетевому администратору регистрировать все действия пользователей в Internet, ограничивать доступ к некоторым сайтам или вводить временные ограничения на доступ, а также кэшировать непосредственно на proxy-сервер часто посещаемые сайты, что позволяет остальным пользователям получать ту же самую информацию намного быстрее.

Для каждого из приложений, необходимых пользователям локальной сети, в межсетевой защите может быть предусмотрен индивидуальный proxy-сервер, как показано на рис. 3.1.

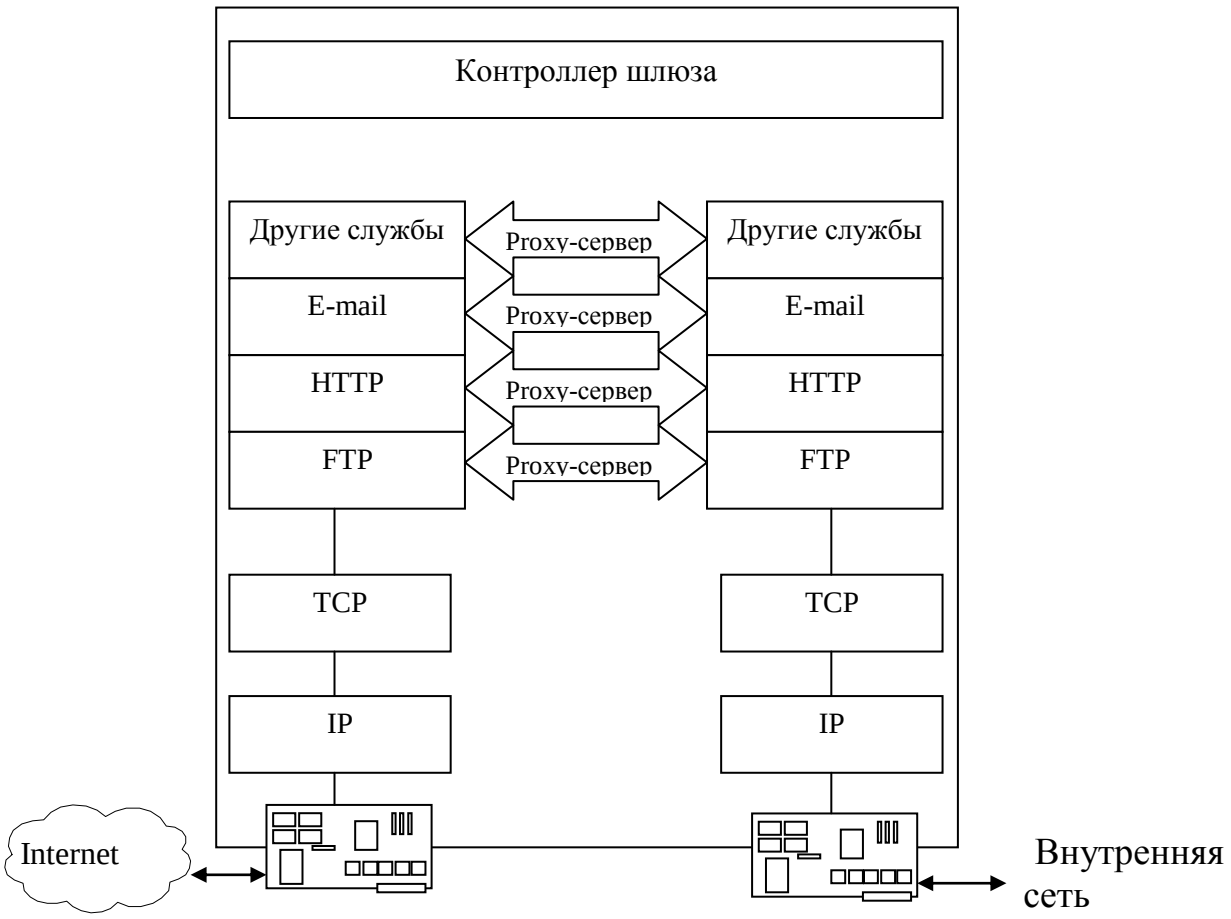


Рис. 3.1. Предоставление proxy – сервером индивидуальных шлюзов для нескольких приложений.

Наиболее популярными на сегодняшний день являются такие прикладные программы как WinProxy и Wingate..

Proxy под управлением Wingate. Wingate был создан для облегчения доступа в Internet. Он может использоваться в любом сетевом окружении, использующем протокол TCP/IP. Wingate управляет доступом к сервисам Internet, таким как электронная почта и World Wide Web. Wingate может использоваться в Интрасети или корпоративной сети, не имеющих доступа в Internet.

Wingate состоит из двух серверных компонентов и клиентского приложения.

Wingate engine - это сервис, запускаемый на машине соединенной с Internet. Он обеспечивает работоспособность соединения, но невидим для пользователя.

Gatekeeper - это интерфейс для управления и настройки Wingate engine. Wingate Internet Client (WGIC) запускается на клиентской машине и обеспечивает доступ к средствам перенаправления Winsock (Winsock redirection).

Так как, GateKeeper использует протокол TCP/IP для соединения с Wingate engine, то он может быть запущен на любой машине. Это означает, что имеется возможность администрировать Wingate с той машины, на которой Wingate установлен.

Таблица 3.1

Возможности Wingate v.3.0

Gatekeeper	Wingate управляется и настраивается с помощью инструмента удаленного администрирования Gatekeeper.
DHCP Сервер	DHCP автоматизирует конфигурацию клиентов в сети. С авто режимом или ручным режимом, Wingate DHCP конфигурирует IP-адреса и DNS для всех клиентских машин.
DNS Сервер	DNS - сервер обеспечивает достаточные функциональные возможности, чтобы использовать сервер SOCKS для запросов SOCKS4. DNS-сервер Wingate объединен с DHCP-сервером, что позволяет разрешить DNS. Если требуется большее количество функциональных возможностей, может использоваться Mapping proxies, чтобы отправить все запросы DNS к полнофункциональному серверу DNS.
Планировщик	Планировщик позволяет администратору управлять Wingate и системным операциями. Многие операции могут быть

	автоматизированы, включая очистку Log-журнала, выключение Wingate и выполнение командной строки.
Аутентификация клиента	WWW-Proxy Wingate включает инструмент идентификации Java. Это позволяет администраторам требовать идентификации без запуска клиентом Gatekeeper. Когда не аутентифицированный пользователь пытается обращаться к странице сети, отображается 'Sorry' страница и апплет входа в систему.
Поддержка	Wingate может использовать различные подключения к Internet, чтобы дать более широкую пропускную способность и быстрый доступ. Комбинации ISDN и прямых подключений, конфигурируемых на уровне "сервиса", дают полное управление и лучшую производительность.
SOCKS V5 Сервер	Wingate SOCKS сервер совместим с SOCKS 4 и SOCKS 5 (RFC 1928). Поддерживается RFC1929 идентификация, используя базу данных пользователей Wingate. Wingate SOCKS-сервер понимает HTTP. Он может распознать и обрабатывать HTTP-запросы с встроенным WWW-Proxy.
Мощный WWW Proxy	Wingate WWW-Proxy - CERN-совместимый HTTP proxy сервер. Он поддерживает HTTP-запросы, FTP запросы и SSL. Особенности включают способность обработать нормальные (не-proxy) запросы, которые делают его хорошим внешним интерфейсом для существующего WWW-сервера, или даже инструментом автоматического mirroring. Он также позволяет располагать proxy-серверы каскадом через другой proxy или SOCKS4 сервер.
Кэширование HTTP	HTTP Caching - процесс сохранения графики, HTML документов или других файлов из Internet на Wingate машине, что позволяет ускорить поиск.
Типы запросов	Wingate WWW-Proxy настраивается так, чтобы понимать и proxy и не-proxy запросы, позволяя запросам быть обработанными "как обычно" или переназначить их на сервер Internet или страницу, обслуживаемую с диска.

Учет	Превосходный инструмент управления LAN, который позволяет осуществлять контроль в реальном масштабе времени.
Аудит/ Регистрация	Мощные средства ревизии позволяют прослеживать действия пользователей (нарушения лицензии, создание сеанса и завершение, вход в систему, отказы разрешения, и. т.д.)
База данных	База данных пользователей позволяет регистрировать и ревизовать индивидуального пользователя. Могут быть определены группы пользователей, и права доступа назначаются на основании прав группы или пользователя.
Политика безопасности и права	Безопасность Wingate обеспечивается назначением прав пользователей и групп. Имеется множество типов прав, которые можно предоставлять
FTP Proxy	FTP proxy обеспечивает доступ к FTP- серверам. Используется username@hostname метод прохождения firewall. FTP proxy поддерживают non-proxy запросы. Это позволяет proxy действовать как front-end на FTP сервере или каскадом через другой proxy.
XDMA Proxy	Wingate поддерживает Xing Streamworks audio и video клиентов.
Telnet Proxy	Wingate Telnet proxy предоставляет доступ к telnet серверам. Telnet proxy в Wingate поддерживает множество telnet-клиентов, в том числе и под Unix. Telnet также понимает каскадирование
Правила	Сложная система firewall позволяет контролировать загрузку сервера Wingate, включая права на доступ к сервису, системные права доступа, и взаимодействие с группами и пользователями.
Запуск как Сервиса	Wingate работает как сервис под Windows NT Это означает, что Wingate начинает работать когда Windows загружается, вне зависимости от того, какой пользователь вошел в систему.

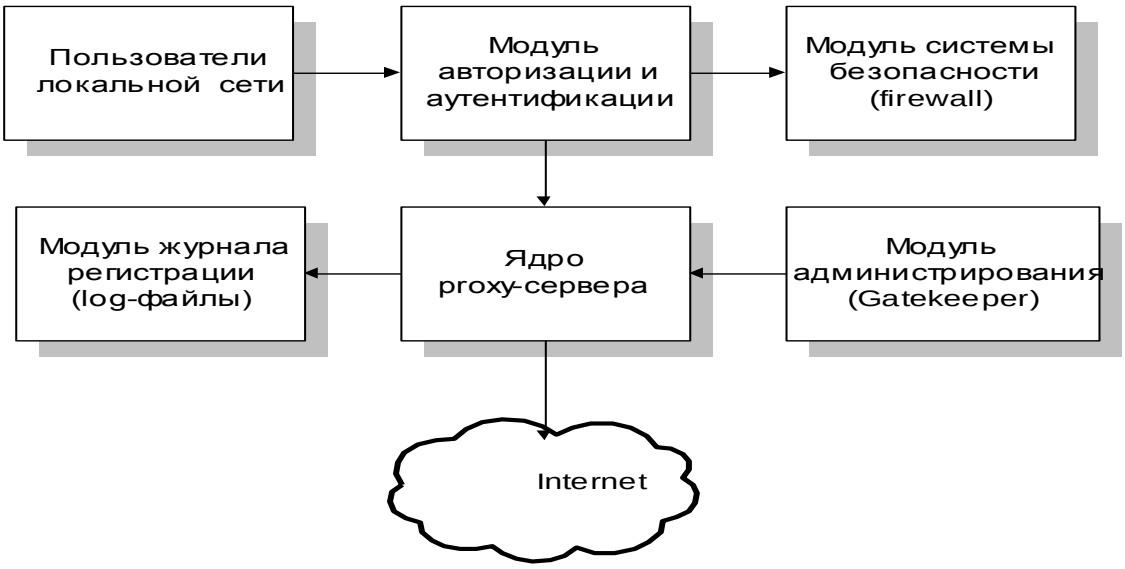


Рис. 3.2. Схема работы proxy-сервера Wingate.

Целью проектирования системы мониторинга является сбор и анализ статистики использования Internet-ресурсов сотрудниками отделов Аппарата Правительства. А также вовремя предотвращение использования его в личных целях. Реализация этой цели достигается решением следующих задач:

- отслеживание объема и содержимого данных получаемых из Internet сотрудниками;
- ведение групповых учетных записей;
- назначение тарифных планов, как отдельным пользователям, так и группам пользователей;
- отключение сразу всех членов группы (обычно сотрудников одного отдела) в случае превышения установленного для группы лимита;
- получение заведующими отделов специальных предупреждений о превышении установленных для их сотрудников лимитов;
- удаленное администрирование через Панель Управления.

Решение вышеперечисленных задач позволит отделу информатизации принимать правильные решения, а Аппарату Правительства - снизить издержки на Internet.

3.2. Алгоритм функционирования программы.

В результате работы proxy-сервера Wingate вся информация о работе пользователя, фиксируется в log-файлах. Это является основным базисом для генерации отчетов и статистики. Извлекаемые данные могут быть представлены в качестве структурированных таблиц, либо в форме отчетов по запрашиваемым данным. Данная информация, также является подтверждением того, что пользователь работал в сети на случай претензий последнего.

Как показала практика последних лет, для достижения этих задач оптимально подходит разработанная фирмой Borland программная среда Delphi.

«Delphi» – это современный программный продукт, позволяющий создавать широкий спектр приложений для среды Microsoft Windows» [11]. Он объединяет в себе высокопроизводительный компилятор с языка ObjectPascal, являющийся объектно-ориентированным расширением структурного языка третьего поколения Pascal, средств наглядного (визуального) создания программ и масштабируемую технологию управления БД. Основное назначение Delphi – служить средством для быстрого создания широкого класса Windows-приложений, включая приложения, отвечающие технологии распределенной обработки данных, называемой технологией клиент-сервер.

Для разработки Windows-приложений Delphi имеет следующие средства:

- высокопроизводительный компилятор

Среда Delphi включает в себя встроенный компилятор, при необходимости можно воспользоваться и пакетным компилятором DCC.EXE.

- объектно-ориентированная модель компонентов

Основным назначением применения в Delphi модели компонентов является обеспечение возможности многократного использования компонентов и создания новых. Для создания Delphi использовались те же компоненты, что входят в состав поставки. Тем не менее, внесенные в объектную модель изменения, в первую очередь, были вызваны необходимостью поддержки технологии визуального программирования. При этом язык остался совместимым с языком Pascal, поддерживаемым компилятором BorlandPascal 7.0

-быстрая среда разработки (RAD)

Среда Delphi содержит полный набор визуальных средств для быстрой разработки приложений, поддерживающих как создание пользовательских интерфейсов, так и обработку корпоративных данных (с использованием соответствующих средств). Использование библиотеки визуальных компонентов (VCL) и визуальных объектов для работы с данными позволяет создавать приложения с минимальными затратами на непосредственное кодирование. При этом компоненты, включенные в состав Delphi, максимально инкапсулируют вызовы функций Windows API, тем самым облегчая процесс создания программ.

-расширяемость

«Delphi является системой с открытой архитектурой, что позволяет дополнять ее новыми средствами и переносить на различные платформы» [11].

-средства для построения БД

Delphi поддерживает практически все форматы существующих реляционных таблиц. Объекты БД в Delphi основаны на SQL и включают в себя полную мощь Borland DataBase Engine.В состав Delphi также включен Borland SQL Link, поэтому доступ к СУБД Oracle, Sybase, Informix и InterBase происходят с высокой эффективностью. Кроме того, Delphi

включает в себя локальный сервер InterBase, для того, чтобы можно было разрабатывать расширяемые на любые внешние SQL-серверы приложения в онлайновом режиме. Разработчик в среде Delphi, проектирующий информационную систему для локальной машины может использовать для хранения информации файлы формата .dbf (как в dBase и Clipper) или .db (Paradox). Если же он будет использовать локальный InterBase for Windows 4.2 (и выше), то его приложения безо всяких изменений будут работать и в составе большой системы с архитектурой «клиент-сервер».

Итак, Delphi – это продукт, позволяющий создавать широкий спектр приложений для Windows. Среда Delphi включает в себя полный набор визуальных средств для быстрой разработки приложений, поддерживающих как создание пользовательских интерфейсов, так и таблиц базы данных. Библиотека классов, входящих в Delphi, содержит около 140 классов, инкапсулирующих различные группы функций Windows API. Delphi является системой с открытой архитектурой, что позволяет дополнять ее новыми средствами, и переносить на различные платформы. Модернизированное ПО ОПВ включает в себя базу данных, для управления которой вполне подходит InterBase Server, разработанный той же фирмой. Производительность и возможности сервера превышают требования данного проекта. При этом InterBase Server условно бесплатен и доступен.

Выходные данные.

Выходная информация представляет собой файлы следующих типов: HTML, EXL, DOC.

Система генерирует следующие виды отчетов:

- сводный отчет;
- отчеты по месяцам, неделям и дням;
- сводные отчеты дням и часам;
- отчеты по пользователям;

- отчеты по IP адресу;
- отчеты о сервисах.

Информационная система мониторинга реализована в виде двух модулей: «генерации отчетов» и «модуля контроля».

1. Генерация отчетов основана с применением компонент Fast Report, и Export Strings которые позволяют быстро создавать отчеты, обрабатывать большое количество информации. А также экспортировать отчеты в Microsoft Excel, Microsoft Word и HTML.

2. Модуль контроля разбит на две части:

- управление Wingate осуществляется через системный реестр Windows;
- подпрограмма которая отслеживает время, пройденное с момента входа пользователя в сеть Internet, до его выхода. А также реализованы API функции Application Programming Interface (что можно приблизительно перевести как "Интерфейс программирования для приложений"), с помощью которых осуществляется связь с приложением Wingate и системой Windows.

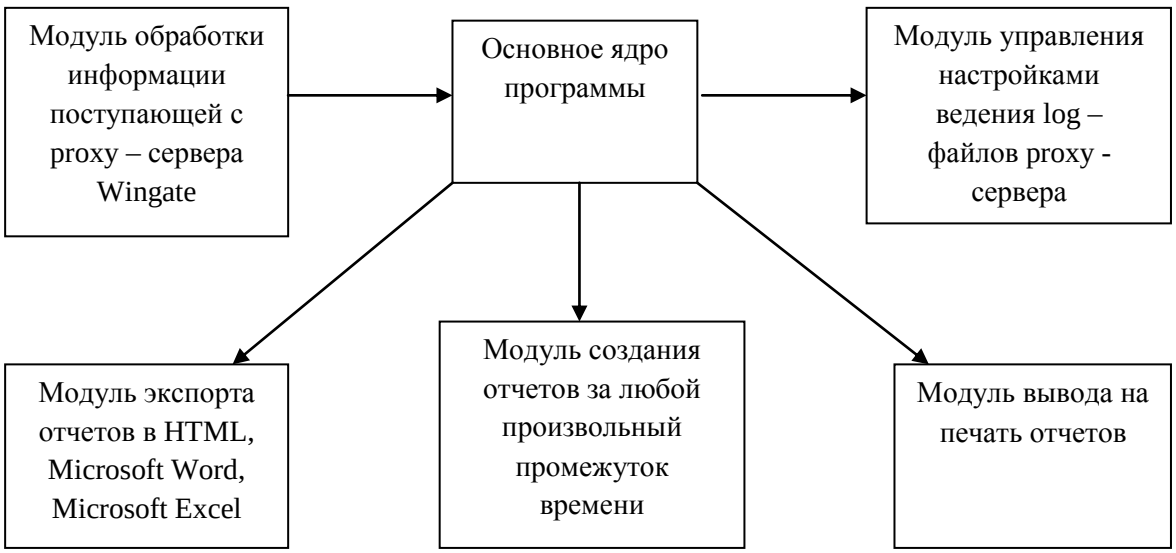


Рис. 3.3. Структурная схема работы программы мониторинга.

Алгоритм функционирования программы можно представить в виде следующей блок схемы. (рис. 3.4).

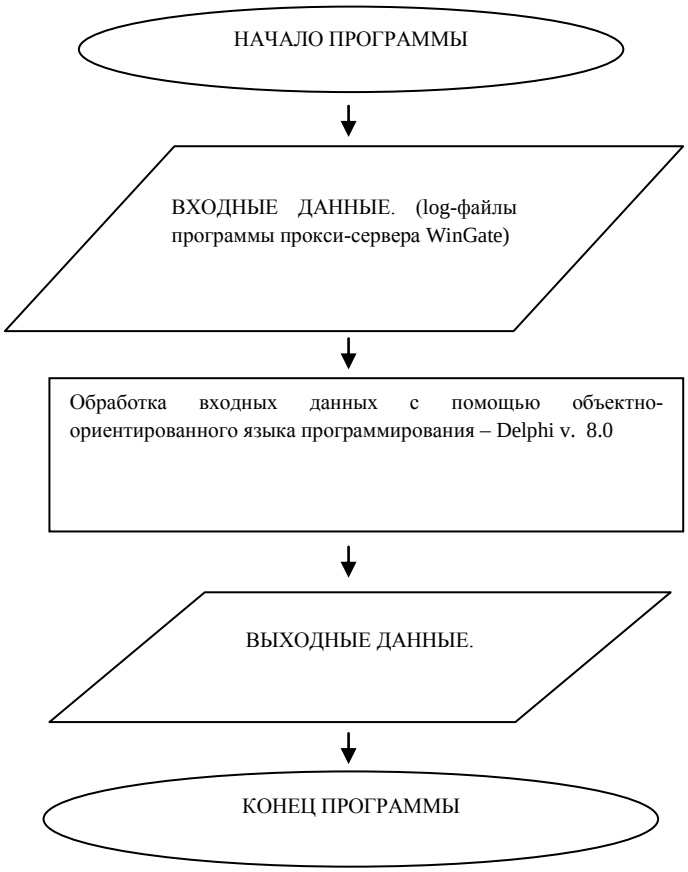


Рис. 3.4. Алгоритм функционирования программы.

3.3. Структура программы.

Программа состоит из нескольких логически связанных между собой блоков, которые отражены в главной форме.

Для корректной работы программы мониторинга необходимо настроить ее.

Для этого нужно выбрать в главном меню «Настройки».

Форма «Настройки» содержит несколько закладок:

- Лог файлы.
- Денежные единицы.
- Лимиты.
- Задачи.

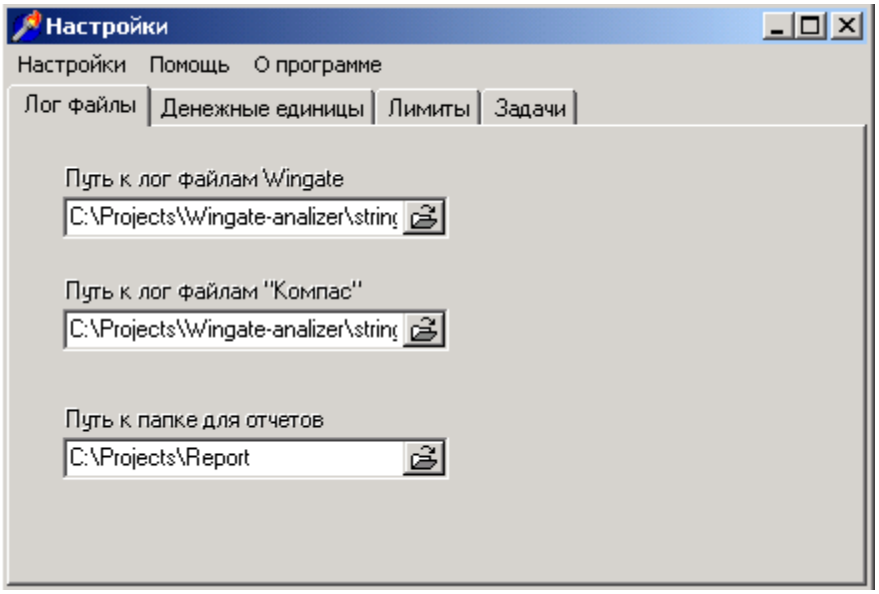


Рис. 3.5. Закладка «Log файлы».

В закладке «Log файлы» указывается путь где находятся журналы регистрации генерируемые proxy-сервером Wingate. А также путь куда будут поступать отчеты генерируемые самой программой.

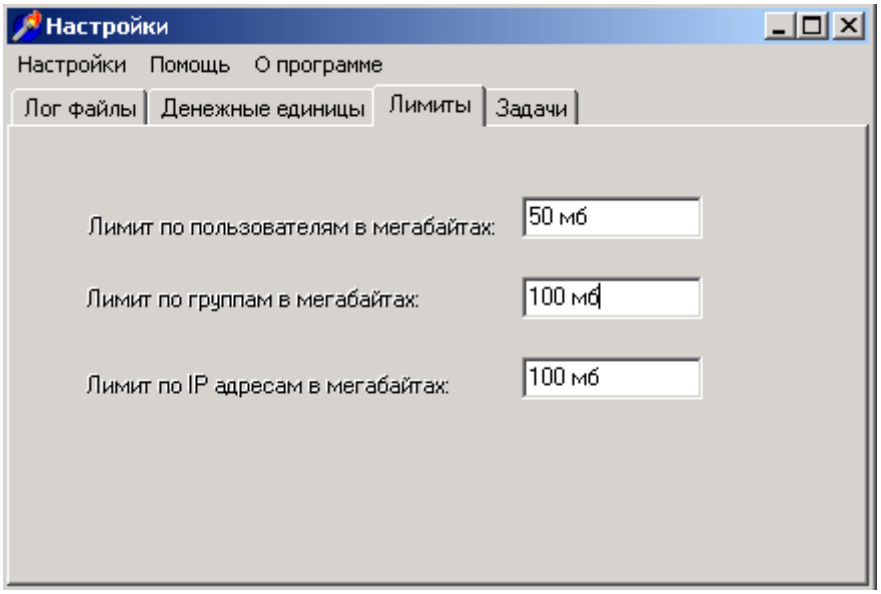


Рис. 3.6. Закладка «Лимиты».

В закладке «Лимиты» задается количество трафика выделяемого на пользователя Internet-ресурсов.

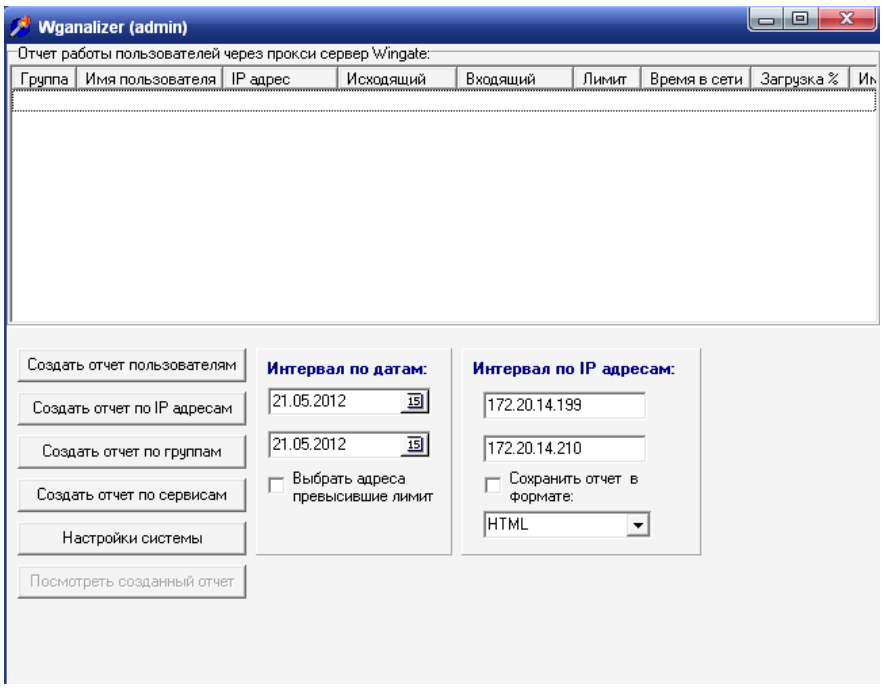


Рис. 3.7. Форма «Отчеты»

Форма «Отчеты» содержит графы:

- Группа.
- Имя пользователя.
- IP адрес.
- Входящий трафик.
- Исходящий.
- % загрузки.

Позволяет создавать необходимый отчет в необходимом формате (HTML, Word, Excel. Text).

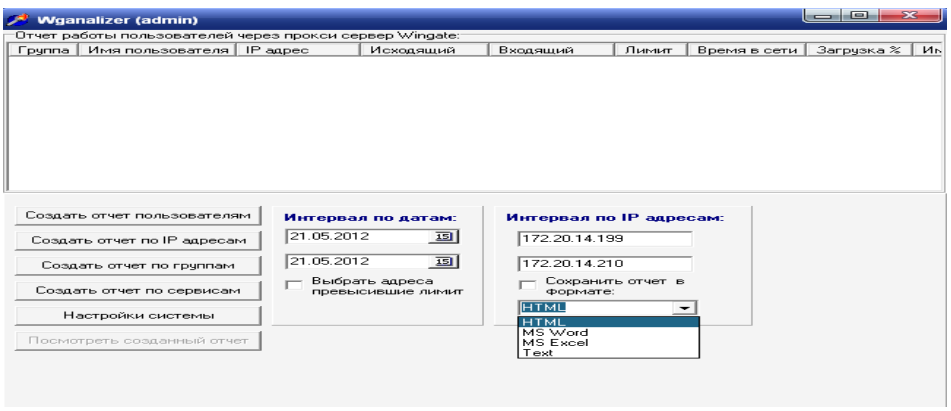


Рис. 3.8. Форма «Отчеты». Выбор формата.

Также позволяет выбрать интервал по датам.

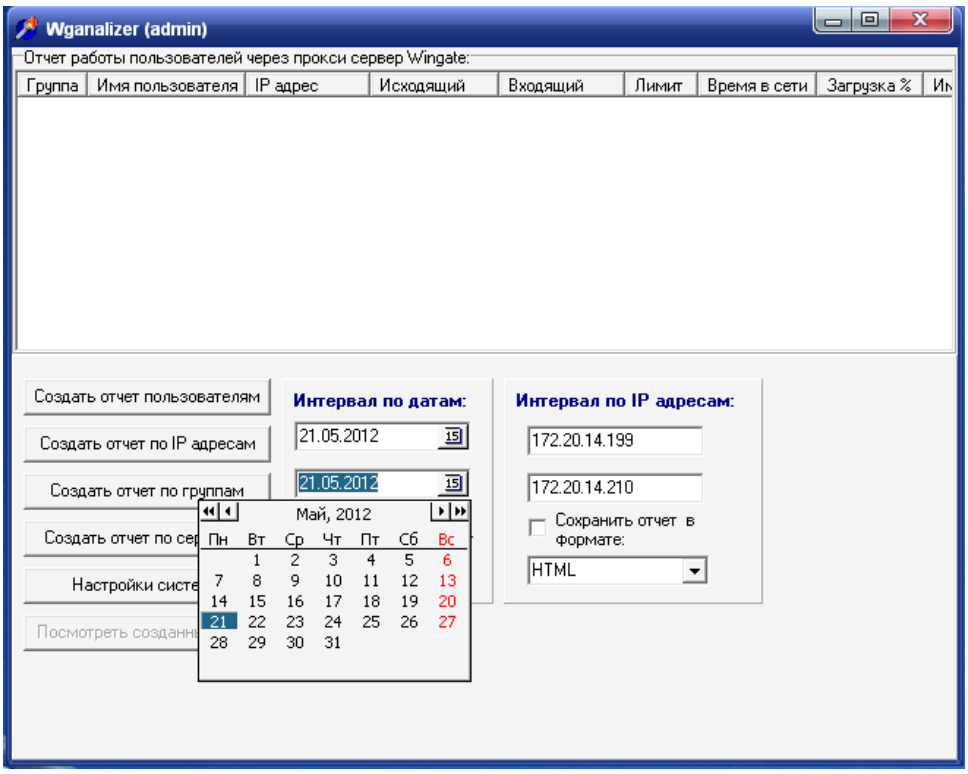


Рис. 3.9. Форма «Отчеты». Выбор даты.

Генерируемые отчеты:

- Отчет по IP адресам;

Отчет по IP адресам: 192.168.0.10, 192.168.0.11, 192.168.0.12, 192.168.0.13, 192.168.0.15, 192.168.0.17,
Период: 01.01.2012 to 19.05.2012 14:57:02

ТРАФИК ПО IP

IP адреса	Исходящий	Входящий	Время в сети	Загрузка %
192.1680.12	74.17 MB	226.60 MB	189085	51.28
192.1680.13	4.41 MB	93.07 MB	30160	16.62
192.1680.11	4.56 MB	88.08 MB	23961	15.79
192.1680.17	3.33 MB	58.52 MB	18552	10.54
192.1680.10	1.63 MB	28.29 MB	9786	5.1
192.1680.15	333.42 Kb	3.58 MB	999	0.67
Всего	88.41 MB	498.15 MB	271543	100

Рис. 3.10. Отчет «Отчет по IP адресам».

- Отчеты по группам и по пользователям;

Отчет по группам: Administrators,"Backup Operators",Guests,"NetShow Administrators","Power Users",Replicator,Users
Период: 01.01.2012 по 19.05.2012 14:58:02

ТРАФИК ПО ГРУППАМ

Группа	Исходящий	Входящий	Лимит, MB	Превышение	Время в сети	Загрузка %
Administrators	4.95 MB	86.79 MB	0 MB(???)	86.79 MB	28331	23.37
Guests	74.17 MB	226.60 MB	0 MB(???)	226.60 MB	188035	76.62
Power Users	2.24 Kb	19.64 Kb	0 MB(???)	19.64 Kb	7	0.01
Всего	79.12 MB	313.41 MB	0 MB	313.41 MB	216423	100

ТРАФИК ПО ПОЛЬЗОВАТЕЛЯМ

Имя пользователя	Исходящий	Входящий	Время в сети	Загрузка %
User6	74.17 MB	226.60 MB	188035	76.62
User2	3.33 MB	58.52 MB	18552	15.76
User3	1.62 MB	28.27 MB	9647	7.61
User9	2.24 Kb	19.64 Kb	7	0.01
User1	1.73 Kb	1.36 Kb	132	0
Всего	79.12 MB	313.41 MB	216423	100

Рис. 3.11. Отчеты «Отчеты по группам и по пользователям».

- Отчет по временным интервалам;

Отчет по пользователям:
Период: 01.01.2012 по 19.05.2012 14:58:02

ТРАФИК ПО ВРЕМЕННЫМ ИНТЕРВАЛАМ

Интервал	Исходящий	Входящий	Время в сети	Загрузка %
Понедельник	44.83 MB	149.36 MB	89035	33.33
Вторник	9.17 MB	158.99 MB	45316	28.67
Среда	18.29 MB	59.50 MB	67145	13.26
Четверг	4.45 MB	53.10 MB	17760	9.81
Пятница	2.88 MB	47.19 MB	25348	8.54
Суббота	7.60 MB	24.50 MB	19611	5.47
Воскресенье	1.20 MB	5.51 MB	7328	1.34
Всего	88.41 MB	498.15 MB	271543	100

Рис. 3.12. Отчет «Отчет по временным интервалам».

Выводы по третей главы

1. Показана целесообразность применения Proxy-серверов для организации системы мониторинга безопасности.
2. С использованием Proxy-серверов в данной работе разработаны алгоритм и программный модуль мониторинга безопасности на примере использующих Internet-ресурсов, позволяющий получить статистические данные о сетевом трафике.

ЗАКЛЮЧЕНИЕ

Развитие информационных систем сопровождается возникновением все новых и новых угроз. Поэтому развитие аппаратных и программных средств мониторинга безопасности КС не только не отстает, но иногда даже и предвосхищает возникновение новых угроз, уменьшая риски для защищаемых информационных систем.

Использование систем мониторинга безопасности с каждым днем становится все более масштабным, в связи с этим растет актуальность описанных задач по защите сетей от атак, контролю распространения вирусов и несанкционированной сетевой активности пользователей, снижению нерационального использования ресурсов.

Основными результатами работы являются:

1. Рассмотрены методы защиты ИКС, сбор и анализ трафика для выявления вредоносных и нежелательных объектов и разработки комплексной системы мониторинга безопасности ИКС.
2. Рассмотрены методы мониторинга безопасности, решающие проблемы непрерывного контроля компьютерных сетей, обнаруживая при этом внутренние и внешние воздействия на ресурсы компьютерных сетей.
3. Выполнен анализ существующих аппаратно-программных средств мониторинга безопасности для определения основных компонентов непрерывного контроля таких, как сетевые сканеры, которые позволяют обнаруживать уязвимости до их применения.
4. Предложен метод мониторинга безопасности при функционировании инфокоммуникационной системы, что позволяет при анализе параметров мониторинга учитывать характеристики загрузки вычислительных ресурсов, параметров уязвимостей и защищенности.
5. Разработаны алгоритм и программный модуль мониторинга безопасности на примере использования Internet-ресурсов, позволяющий получить статистические данные о сетевом трафике.

Список литературы:

1. Выступление Президента Республики Узбекистан Ислама Каримова на открытии международной конференции «Подготовка образованного и интеллектуально развитого поколения – как важнейшее условие устойчивого развития и модернизации страны»
2. Каримов И. А. «Узбекистан по пути углубления экономических реформ» Т.: Узбекистон, 1995 г.
3. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учеб. пособие для вузов.- М.: Горячая линия - Телеком, 2011.- 320 с.
4. Липаев В.В. Тестирование компонентов и комплексов программ.— М.: Синтег, 2010.— 400 с.
5. Черников Б.В. Управление качеством программного обеспечения: Учебник для вузов.— М.: ИНФРА-М, 2011
6. Варлатая С.К., Шаханова М.В. Программно-аппаратная защита информации: учеб. пособие – Владивосток: Изд-во ДВГТУ, 2007. – 318 с.
7. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации.
8. М.: Агентство «Яхтсмен», 1996.
9. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия - Телеком, 2000.
10. Корн Г., Корн Т. Справочник по математике (для научных работников и инженеров). − М.: Наука, 1973. − 832 с.
11. Репин Д.С. Анализ и моделирование трафика в корпоративных компьютерных сетях: дис. канд. техн. наук: спец. 05.13.01 «Системный анализ, управление и обработка информации (промышленность)» / Д.С. Репин. – М., 2008. – 143 с.
12. Крон Г. Тензорный анализ сетей, пер. с англ., род ред. Л.Т.Кузина, П.Г.Кузнецова. – М.: Сов. радио, 1978. – 720 с.

13. Vincent Berk, Annarita Giani, George Cybenko Detection of Covert Channel Encoding in Network Packet Delays. 2005.
14. Myong H. Kang, Ira S. Moskowitz A Pump for Rapid, Reliable, Secure Communication // 1st ACM Conference on Computer & Communications Security. 1993. PP. 119–129.
15. Тарасюк М. В. Адаптивная маскировка скрытых каналов в открытых системах с многоуровневым доступом.
16. Остроухов М. Поговорим о брандмауэрах/ М. Остроухов// КомпьютерПресс. – 2005. - №2. – С. 80-86.
17. F. Baker and P. Savola, "Ingress Filtering for Multihomed Networks," RFC 3704, March 2004.

Интернет ресурсы:

1. www.gov.uz
2. www.tuit.uz
3. www.intuit.uz
4. http://www.loniis.ru/about/
5. http://inf-bez.ru/?p=586
6. http://www.sseu.ru/about/inform/norm/insmonit/
7. http://www.computel.ru/decision/ssb/Monitoring%20IS/
8. http://www.infosec.ru/services/support/outsourcing/monitoring/

ПРИЛОЖЕНИЕ

```
unit Unit1;

interface

uses
  Windows, Messages, SysUtils,shellapi, Classes, Graphics, Controls, Forms, Dialogs,
  StdCtrls, lmdctrl, lmdstdcA, ExtCtrls, EC_Main, EC_TStrings, Mask,
  ToolEdit, lmdcctrl, lmdgroup, RxLogin,Hyperstr;
type
  TForm1 = class(TForm)
    GroupBox1: TGroupBox;
    List1: TLMDListBox;
    Panel1: TPanel;
    Button1: TButton;
    Exp1: TExportStrings;
    Panel2: TPanel;
    Label1: TLabel;
    DateEdit1: TDateEdit;
    DateEdit2: TDateEdit;
    Panel3: TPanel;
    Label2: TLabel;
    Edit1: TEdit;
    Edit2: TEdit;
    Button2: TButton;
    Button3: TButton;
    Button4: TButton;
    Button5: TButton;
```

```
    LMDCheckBox1: TLMDCheckBox;
    LMDCheckBox2: TLMDCheckBox;
    Box1: TComboBox;
    Login1: TRxLoginDialog;
    M1: TMemo;
    LBox1: TListBox;
    Button6: TButton;
    procedure Button1Click(Sender: TObject);
    procedure Button5Click(Sender: TObject);
    procedure FormShow(Sender: TObject);
    procedure Button6Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;
var
  Form1: TForm1;
implementation
uses Unit2;
{$R *.DFM}
procedure TForm1.Button1Click(Sender: TObject);
var i,traff,a,b,a1:longint;
w,st,ss,traf,filen,data,ip,user,gr,traf1,lim,time,file_buf:string;
begin
```

```
file_buf:= form2.patchwg1.Text+'\'+form2.file1.Items[0] ;
m1.Lines.LoadFromFile(file_buf);
case box1.ItemIndex of
  0:
   begin
    exp1.ExportType:=xHTML;
filen:='report.html';
   end;
  1:
   begin
    exp1.ExportType:=xMicrosoft_Word;
filen:='report.rtf';
    end;
  2:
   begin
      exp1.ExportType:=xMicrosoft_Excel;
filen:='report.xls';
   end;
  3:
   begin
      exp1.ExportType:=xText_Tab_Delimited;
filen:='report.txt';
   end;
 end;
//exp1.ExportFile:='strings';
```

```
exp1.ExportFile:=form2.DirectoryEdit1.Text+'\'+filen;

//list1.Items.LoadFromFile('c:\program files\Wingate\logs\logs_all1.txt');

for a:=1 to m1.Lines.Count-1 do

begin

st:=m1.Lines[a];

for b:=1 to length(st) do

begin

if b<18 then

data:=data+st[b];

end;

ReplaceSC(st,#9,DupChr(#32,1),False);// replaces all tabs with 8 spaces.

ReplaceC(st,' ','#');

m1.Lines[a]:=st;

i := 1;

lbox1.Items.clear;

repeat

W := ParseWord(St,'#',I);

if Length(W)>0 then

LBox1.Items.Add(W)

else break;

until True=False;

data:=LBox1.Items[0]+'-'+LBox1.Items[1];

user:=LBox1.Items[3];

ip:=LBox1.Items[2];

if LBox1.Items.Count>5 then
```

```
traf:=LBox1.Items[6] else traf:='0';

if LBox1.Items.Count>9 then begin

traf1:=LBox1.Items[7];

time:=LBox1.Items[10];

end;

if length(form2.Edit1.text)<1 then

lim:=form2.Edit3.text else

lim:=form2.Edit1.text;

if (length(user)<>0) then

if (length(ip)<>0) then

if (length(traf)<>0) then

if (traf[1]<>'S')  then //  showmessage(traf);

if (traf[1]<>'h')  then //  showmessage(traf);

list1.AddLine(['net',user,ip,traf1,traf,lim,time,'','50',data]);

//if a=150 then

//exit;

//showmessage(traf);

//ReplaceSC(st,#9,DupChr(#32,2),False);

//for a1:=1 to length(st) do

//if st[a1]=' ' then

//st[a1]:=';';

end;

button6.Enabled:=true;

for b:=0 to list1.items.Count-1 do begin

ss:=list1.ItemPart(b,4);
```

```
if length(ss)>0 then
if IsNum(ss)= true then
traff:=strtoint(ss)+traff;
//showmessage(ss);
end;
exp1.Strings:=list1.Items;
exp1.Footer.Add('Общий трафик: '+inttostr(traff)+' байт');
exp1.Footer.Add(inttostr(round(traff/1024))+' Кбайт');
exp1.Footer.Add(inttostr(round(traff/1024/1000))+' Мбайт');
exp1.Execute;
end;
procedure TForm1.Button5Click(Sender: TObject);
begin
form2.ShowModal;
end;
procedure TForm1.FormShow(Sender: TObject);
begin
box1.ItemIndex:=0;
dateedit1.Date:=date;
dateedit2.Date:=date;
form2.file1.Directory:=form2.patchwg1.text;
end;
procedure TForm1.Button6Click(Sender: TObject);
begin
ShellExecute(0, 'open', pchar(exp1.ExportFile), '',pchar(exp1.ExportFile), SW_SHOWNORMAL);
```

```
end;

end.

unit Unit2;

interface

uses
  Windows, Messages,shellapi,SysUtils, Classes, Graphics, Controls, Forms, Dialogs,
  Menus, StdCtrls, ExtCtrls, RXClock, ToolEdit, CurrEdit, RXCtrls, Mask,
  ComCtrls, aprstore, lmdcctrl, lmdctrl, lmdeditb, lmdeditc, lmdbredt,
  lmdstdcA, Lmddbctr, FileCtrl;
type
  TForm2 = class(TForm)
    MainMenu1: TMainMenu;
    N1: TMenuItem;
    N2: TMenuItem;
    N3: TMenuItem;
    LogWingate1: TMenuItem;
    OpenDialog1: TOpenDialog;
    N4: TMenuItem;
    N5: TMenuItem;
    Page1: TPageControl;
    TabSheet1: TTabSheet;
    TabSheet2: TTabSheet;
    TabSheet3: TTabSheet;
    TabSheet4: TTabSheet;
    FilenameEdit2: TFilenameEdit;
```

RxLabel1: TRxLabel;

RxLabel2: TRxLabel;

DirectoryEdit1: TDirectoryEdit;

RxLabel3: TRxLabel;

CurrencyEdit1: TCurrencyEdit;

CurrencyEdit2: TCurrencyEdit;

RxLabel4: TRxLabel;

ComboEdit1: TComboEdit;

ComboEdit2: TComboEdit;

RxLabel5: TRxLabel;

RxLabel6: TRxLabel;

RxLabel7: TRxLabel;

FilenameEdit3: TFilenameEdit;

RxLabel8: TRxLabel;

DateEdit1: TDateEdit;

RxClock1: TRxClock;

RxLabel9: TRxLabel;

RxLabel10: TRxLabel;

Edit1: TEdit;

Edit2: TEdit;

Edit3: TEdit;

AutoPropertiesStore1: TAutoPropertiesStore;

patchwg1: TDirectoryEdit;

RxLabel11: TRxLabel;

RxLabel12: TRxLabel;

```
    RxLabel13: TRxLabel;
    SpinEdit1: TLMDSpinEdit;
    SpinEdit2: TLMDSpinEdit;
    Label1: TLabel;
    Label2: TLabel;
    CheckBox1: TCheckBox;
    File1: TFileListBox;
    procedure LogWingate1Click(Sender: TObject);
    procedure N3Click(Sender: TObject);
    procedure RxClock1GetTime(Sender: TObject; var ATime: TDateTime);
    procedure FormCreate(Sender: TObject);
    procedure patchwg1AfterDialog(Sender: TObject; var Name: String;
      var Action: Boolean);
    procedure patchwg1Change(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;
var
  Form2: TForm2;
implementation

uses Unit1;
{$R *.DFM}
```

```
procedure TForm2.LogWingate1Click(Sender: TObject);
begin
if OpenDialog1.Execute then
//OpenDialog1.FileName:=
form1.M1.Lines.LoadFromFile(OpenDialog1.FileName);
end;
procedure TForm2.N3Click(Sender: TObject);
begin
page1.ActivePage:= TabSheet2;
end;
procedure TForm2.RxClock1GetTime(Sender: TObject; var ATime: TDateTime);
var
  dTime: TDateTime;
begin
try
//Rxclock1.AlarmMinute:=44;
if spinedit1.Value=0 then
spinedit1.Text:='00';
if spinedit2.Value=0 then
spinedit2.Text:='00';
dtime:=StrToDateTime('30.12.1899 '+spinedit1.Text+':'+spinedit2.Text+':02');
Label1.Caption := DateTimeToStr(dtime);
Label2.Caption := DateTimeToStr(Atime);

if not checkbox1.Checked then begin
```

```
if dateedit1.Date=date then

if Label1.Caption=Label2.Caption then

ShellExecute(0, 'open', pchar(FilenameEdit3.FileName), '',pchar(FilenameEdit3.FileName),
SW_SHOWNORMAL);

end else begin

if Label1.Caption=Label2.Caption then

ShellExecute(0, 'open', pchar(FilenameEdit3.FileName), '',pchar(FilenameEdit3.FileName),
SW_SHOWNORMAL);

end;

except

Application.MessageBox('=хяЁртшы№эущ ЇюЁьрЄ фрЄv шыш тЁхьхэш!', '¦ююярё',
MB_OK+MB_ICONHAND+MB_DEFBUTTON1+MB_APPLMODAL);

end;

end;

procedure TForm2.FormCreate(Sender: TObject);

begin

dateedit1.date:=date;

//dateedit1.text:='01.01.01';

end;

procedure TForm2.patchwg1AfterDialog(Sender: TObject; var Name: String;

  var Action: Boolean);

begin

if Action = true then

form2.file1.Directory:=form2.patchwg1.text;

end;

procedure TForm2.patchwg1Change(Sender: TObject);
```

```
begin

form2.file1.Directory:=form2.patchwg1.text;

end;

end.
```