ПРОБЛЕМЫ БЕЗОПАСНОСТИ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ

ISBN 966-7418-41-3

Седова В.В., к.э.н. ст. преп. каф. ВЭДП
Надтока Б.А., магистрант каф. системы программного управления, немецкого технического факультета

Представлена постановка проблемы ценности информационных ресурсов с точки зрения безопасности использования. Описаны основные подходы к решению этой проблемы при использовании информации в LAN, а также вопросы интеграции локальной сети с глобальной вычислительной сетью Internet. Определены основные обязанности руководителя в области технической и организационной деятельности по обеспечению безопасной работы сети предприятия (структурного подразделения).

In this article the problems of value of informational resources have been presented from the security point of view. The main approaches to resolve these problems in use of information in LAN have been described. Also the questions of integration of LAN with the global computer network Internet. The principle obligations of the manager in the field of technical and organisational activities to provide operational sequrity of the enterprise network (organisational subdevision) have been defined.

Информационная технология, трансформировавшая традиционные рынки, существовавшие способы обмена и работы с информационными ресурсами, создала новые организационные структуры, сделав бизнес более эффективным и безопасным, а работу специалистов более продуктивной, превратила персональный компьютер в основной рабочий инструмент экономиста и инженера-исследователя.

Сегодня появляются всё новые аспекты применения возможностей информационной технологии в бизнесе, государственном секторе, учебных заведениях, исследовательских центрах и других общественно-экономических институтах с тем, чтобы повысить их конкурентоспособность и реагируемость на изменения, происходящие во внешнем мире.

Это предполагает рассмотрение информации как такого же важного актива, как и любого другого вида актива из баланса предприятия или организации. Цена своевременной и достоверной информации неизмеримо возрастает в настоящее время, тем более учитывая ее быстрое устаревание и изменчивость. На самом нижнем уровне успех в бизнесе определяется привлечением, удовлетворением и удерживанием покупателей. Потребители оценивают способность взаимодействовать с поставщиками для того,

чтобы безопасно работать с заказом, формулировать запросы, получать своевременное и качественное обслуживание и иметь обратную связь, служащую ключевой частью цикла планирования компании. Страхование операций становится необходимым для сетевой торговли, продаж информации по сети и некоторых других приложений, весьма распространенных при развитой технологии.

Фактом является то, что лишь небольшое количество организаций эффективно управляют информационным активом внутри их оргструктуры. Различная информация хранится на различных системах, которые не могут общаться друг с другом. Единственным выходом в этой ситуации представляется создание высокоунифицированных систем, имеющих достаточно прозрачную связь с внешним миром. Решения в этой области базируются на создании внутренних intranet-сетей и внешних экстрасетей, (связывающих производителей, поставщиков и заказчиков), имеющих доступ к ресурсам Internet.

Естественно, что при работе в такой системе вопросы информационной безопасности выступают на передний план. Как было показано выше, информация в настоящее время - это наиболее важный, даже скорее - самый дорогостоящий, а к тому же и наиболее уязвимый элемент в структуре организации. Поэтому, при организации надежной, хорошо структурированной, правильно функционирующей и обязательно защищенной от внешнего вмешательства информационной системы, следует прежде всего учитывать аспекты конфиденциальности и защищенности коммерческой, научно-технической и организационно-распорядительной информации. При этом поддержка безопасного использования информации включает следующий ряд функций, которые должны быть выполнены:

- аутентификацию - проверка личности пользователя компьютера или всей сети;
- управление доступом – проверка и обеспечение разрешенного доступа пользователю компьютерной сети, следующая за установлением личности пользователя;
- обеспечение целостности данных – проверка содержимого массива данных (сообщения, файла, программы) для случайно или намеренно внесенных изменений недозволенным способом;
- гарантирование конфиденциальности информации – защита от несанкционированного содержания данных;
- защита от отказа в отправке или получении массива данных отправителем или получателем.

Существует большое разнообразие методов проникновения в информационную систему организации с целью получить секретную информацию или же с целью нанести вред либо уничтожить некоторые файлы системы. Эти способы "проникновения в систему" предполагают как самые примитивные, типа злоупотребления доверием пользователей, выявление

пароля и др., так и современные профессиональные способы сегодняшних хакеров.

Поскольку современная информационная система организации предполагает своей неотъемлемой частью интеграцию в единую компьютерную сеть Internet, то и предоставляет, таким образом, информационное окно вашей локальной сети или персонального компьютера как добросовестным пользователям, так и потенциальным "охотникам" за информацией. При подключении локальной сети к Internet используется брандмауэр, который представляет собой либо аппаратное устройство, например маршрутизатор, либо работающую на компьютере программу, которая создает барьер между Internet и LAN, иными словами выходит в Internet от имени локальной сети. Брандмауэры предотвращают несанкционированный доступ к корпоративной сети, ограничивают входящий, а часто и исходящий трафик, аутентифицируют пользователей и регистрируют информацию о трафике, как приходящем, так и исходящем.

Современное программное обеспечение для работы с Internet - программы просмотра (браузер) - имеют функциональный набор средств защиты. Эти средства защиты, встроенные в сам браузер Internet, обеспечивают определенное невмешательство через программу просмотра, например, к системным файлам.

В одних случаях воздействие на систему происходит безболезненно, а в других могут возникнуть серьезные проблемы. Решения по этому вопросу требуют единого подхода, что облегчит передачу защищенной информации по World Wide Web и упростит ее использование для потребителей. Объединив два передовых стандарта безопасности операций - Secure HTTP от Enterprise Integration Technologies и SSL (Secure Sockets Layer) от Netscape - в единый пакет, можно получить подход, обеспечивающий взаимодействие приложений, т.е. приложения могут безопасно связываться, даже если они предоставлены различными организациями с разнообразными сетевыми решениями.

SSL - Secure Sockets Layer - представляет собой открытый протокол безопасности со свободным доступом, который удобен для использования в Internet и других сетях TCP/IP. Его можно использовать с протоколами уровня приложений, такими как HTTP, FTP, Gopher, telnet и многими другими (включая еще не разработанные протоколы). SSL обеспечивает защищенную процедуру идентификации узлов, которая применяется для инициализации соединения TCP/IP. Клиент и сервер используют эту процедуру для выработки соглашения об уровне безопасности, который будет поддерживаться при обмене данными между ними. Этот же протокол соблюдает все формальности процедуры аутентификации. После инициализации соединения SSL используется только для кодирования и декодирования передаваемого потока байтов. Таким образом, данные, которыми обмениваются клиент и сервер, передаются в полностью зашифрованном

виде, например стандартные "анкетные" данные (номер кредитной карточки), информация для процедуры идентификации HTTP (имена и пароли пользователей), URL, по которым обращаются клиенты, и данные, которые пересылает сервер по запросам клиентов.

Сейчас, когда сети становятся более глобальными, объединяющие огромное количество предприятий, коммерческих организаций, банков, необходимо, чтобы внутри системы стратегия безопасности выполнялась прежде всего конечным пользователем. Традиционно конечные пользователи не заботятся о защите своих данных и, как правило, в недостаточной степени удовлетворяют требуемой технической квалификации. Как результат, - и необходимость - системные администраторы устанавливают процедуры для защиты данных без вовлечения в этот процесс пользователей. Часто это может привести и к негативным последствиям. Решение состоит в организации интегрированной информационной системы, в которой участвуют как конечные пользователи, так и системные профессионалы с использованием современных систем информационного менеджмента, повышающих эффективность и, определенно, функциональность информационной среды.

Одним из возможных интеграционных решений по информационному менеджменту для организации является набор программных продуктов компании Lotus. Там, где intranet и Internet имеют соприкосновение в области деловой активности организации, Lotus предлагает технологию для того, чтобы обеспечить конфиденциальность и единость данных также хорошо, как систему для установления подлинности отдельных людей и компьютеров. Lotus Notes - один из лидеров группового программного решения, которое интегрирует наиболее надежную систему сообщений (клиент/сервер), групповое программное обеспечение и Internet.

Какие же технологии имеются сегодня на достаточно продвинутом уровне в области Internet-безопасности? Определенно, как и в локальной сети, так и в Internet, одним из направлений является инкрипция сетевого трафика. Другими элементами технологии являются криптографическая аутентификация.

Нельзя также не согласиться с экспертами в том, что протокол SKIP (Simple Key management Protocol) – протокол управления криптоключами в интрасети, ставший стандартом Internet, является развитием в области шифрования трафика. В основе протокола лежит криптография открытых ключей. У SKIF существует ряд уникальных особенностей в системах шифрования трафика, как например универсальность, открытость в смысле взаимодействия с другими системами безопасности и другие. Перспективные разработки в обеспечении безопасности локальных сетей представляют устройство коллективной защиты локальной сети SKIPBridge. Устройство SKIPBridge представляет собой систему, устанавливаемую на интерфейсе внутренняя/внешняя сеть (локальная сеть/коммуникационный

провайдер). Устройство обеспечивает защиту информационного трафика, направляемого из внутренней сети во внешнюю на основе протокола SKIP, а также фильтрацию и дешифрирование трафика, поступающего из внешней сети во внутреннюю. IP-пакеты, принимаемые из внешней сети обрабатываются протоколом SKIP. Пакеты, которые прошли фильтрацию, при помощи IP передаются программному обеспечению SKIPBridge, которое производит решение задач административной безопасности, а затем – операционной системе устройства SKIPBridge, которая маршрутизирует приходящие пакеты на адаптер внутренней (локальной) сети.

Одним из продвинутых решений в области аппаратной защиты локальных сетей является устройство SunScreen. Это специализированная система защиты, разработанная компанией Sun Microsystems, решающая задачи развитой фильтрации пакетов, аутентификации и обеспечение конфиденциальности трафика. Данное устройство работает на основе мощного процессора SPARC в специальной усеченной версии ОС Solaris, из которой изъяты функции низкоуровневой обработки пакетов IP. SunScreen не имеет адреса IP, поэтому «невидим» из внешней сети и не подвержен непосредственному вторжению.

Рабочая конфигурация системы предполагает несколько Ethernet-адаптеров, к которым подключаются независимые сегменты локальной сети и коммуникационный провайдер. Для каждого сегмента обеспечивается настройка системы безопасности путем задания сложного набора правил фильтрации пакетов (по направлению распространения, по адресам отправителя/получателя, про протоколам, по времени суток и т.д.). В свою очередь, другим важным аспектом SunScreen является поддержка протокола SKIP, что с, одной стороны, используется для обеспечения безопасности работы, управления и конфигурирования системы SunScreen, а с другой стороны – позволяет организовать SKIP-защиту пользовательского графика. Использование протокола SKIP в Screen-системах позволяет инкапсулировать весь внешний трафик защищаемых локальных сетей в SKIP. При этом исходные IP-пакеты могут помещаться в блоки данных SKIP-пакетов, а сетевые адреса всех узлов внутренней сети могут быть заменены на некоторые виртуальные адреса, отвечающие во внешней сети Screen-устройствам (адресная векторизация). В результате весь трафик между защищаемыми локальными сетями может выглядеть извне только как полностью шифрованный трафик между узлами Screen-устройств. Вся информация, которая может быть в этом случае доступна внешнему наблюдателю, - это временная динамика и оценка интенсивности трафика, которая может маркироваться путем использования сжатия данных и выдачи «пустого» трафика.

Еще одним решением, а точнее следующим шагом к безопасности, является применение смарт-карт. Этот вопрос очень важен в смысле электронной идентификации, поскольку лишь только смарт-карта, являясь фи-

зическим объектом, может выступать потенциальным носителем безопасности, т.к. как только смарт-карта похищена, утеряна и т.д., пользователь сразу же осведомлен об этом, и ему следует предпринять соответствующие действия.

Смарт-карта - это карточка, подобная по размеру сегодняшним платежным пластиковым карточкам, которая имеет чип, встроенный в нее. Посредством добавления чипа в карту, она становится смарт-картой, способной служить многим различным пользователям. В качестве устройства контроля доступа смарт-карты делают личную и деловую информацию доступной только разрешенным пользователям. Смарт-карта обеспечивает переносимость данных, безопасность и удобство в использовании.

Работа смарт-карт основана на архитектуре клиент-сервер. С помощью удаленного программного клиента устанавливается соединение с центральным сервером, естественно, через небезопасную сеть, а сервер отвечает запросом на опознавание. Клиент, в свою очередь, передает его смарт-карте через устройство считывания смарт-карт. Смарт-карта формирует цифровую подпись запроса на опознавание с помощью секретного ключа, который не может быть подвержен влиянию вируса или потенциально угрожающей ОС клиента. Смарт-карта возвращает через клиента подписанный ответ серверу. Последний и осуществляет проверку подписи.

International Organization for Standardisation (IS/O) - Международная Организация по Стандартизации - приняла стандарты для смарт-карт. Эти стандарты были разработаны для использования различными предприятиями. Отдельные предприятия сегодня разрабатывают соответствующие версии этих стандартов ISO для того, чтобы поддержать их собственные специфические приложения смарт-карт. Они проектируются таким образом, чтобы соответствовать стандартам, выпущенным ISO. Цель - обеспечить единообразие стандартов для смарт-карт как элементов контроля безопасности, которые позволят организовать взаимодействие смарт-карт среди широкого числа предприятий.

Следует также отметить, какие элементы безопасности являются абсолютно необходимыми при работе через Internet. Несмотря на то, что существует специфика в той или иной организации, ответом служат следующие основные технологии: контроль доступа, криптографическая аутентификация, шифрование взаимодействий, осуществляемых через сеть Internet, цифровые подписи и др. Предлагаемые на современном уровне решения в области электронных взаимодействий должны непременно использовать их.

Еще одна потенциальная угроза безопасности - компьютерные вирусы. Угроза информации может возникнуть не только в том случае, если недобросовестный потребитель может использовать ее, но и в случае уничтожения, когда, например, наиболее важная электронная информация становится объектом воздействия компьютерного вируса. Этот же факт

следует рассматривать и при организации работы с Internet в случае использования программного обеспечения, полученного из Сети - это пример косвенного воздействия.

Построение современных систем электронного коммерческого взаимодействия, а также более или менее сложных систем статистики и мониторинга через Internet, а точнее их реализация, предполагает использования кроссплатформенного языка программирования Java. Являясь языком программирования под Internet, а теперь и в сочетании с динамическим HTML, он позволяет создавать мощные коммерческие как клиентские приложения, так и серверные программы. Кроме создания движущихся элементов на экране, язык превратился в средство реализации технологии принудительного распространения программного обеспечения и даже электронной коммерции.

Коды Java выполняются локально, на машинах конечных пользователей, подвергая эти машины опасности воздействия. Java-апплеты и Java-приложения при создании коммуникационного взаимодействия клиент-сервер используют гнездовые соединения. Они также имеют некоторые возможности воздействия на операционную систему клиента. Однако, создание грамотных приложений, написанных на Java и использующих специальные объектно-ориентированные методы программирования (класс Sequrity Manager), позволят создать и применить в дополнению к другим методам защиты коммуникаций и работы приложения еще и внутренние механизмы системной защиты путем реализации соответствующего объектного класса.

Создание требуемого интерактивного пользовательского интерфейса с помощью Java-клиентов позволяет значительно повысить функциональность и гибкость коммуникационного взаимодействия между клиентом и серверным приложением, используя ресурсы машины-клиента и организовывая передачу актуальной информации как серверному приложению с браузера клиента, так и наоборот. Речь идет как о котировках акций на бирже, так и о обновлении текущего состояния банковского счета. Диапазон применения Java для коммерческих приложений очень велик: от элементарного обновления курса валют до сложнейших систем биржевых продаж и систем мониторинга.

Посмотрим немного вглубь. Прежде всего разработчики пишут исходный код на языке программирования Java. Компилятор преобразует этот код в байт-код Java. Байт-код в форме апплета размещается на странице Web, доступ к которой осуществляется при помощи браузера, рассчитанного на работу с Java. Браузер проверяет код, после чего виртуальная машина Java (Java Virtual Machine, JVM) осуществляет выполнение апплета на клиентской машине. Java с самого начала была задумана как технология, с помощью которой однажды написанная программа могла выполняться на любой платформе. И так как Java может работать в систе-

ме практически любого типа, и поскольку апплеты Java с удаленного сервера выполняются на клиентской машине, JavaSoft, подразделение корпорации Sun, приложило немало усилий к тому, чтобы решить вопросы защиты на уровне языка программирования.

Многие производители любят повторять, что безопасность Java - очевидный вопрос, но создатели языка с самого начала знали, что вопросы защиты будут иметь решающее значение для судьбы предложенной технологии. К сожалению, не все пользователи знают, что как Java, так и ActiveX посылают программный код на клиентский компьютер, где этот код и исполняется. Все так называемые мобильные или переносимые программы попадают непосредственно в клиентскую систему и делают там то, для чего они написаны. Это происходит независимо от желания пользователя, если в установках защиты нет соответствующего запрета.

Вся система безопасности Java строится вокруг так называемой модели безопасности Sandbox (этот термин можно примерно перевести как "ящик с песком"). Эта идея реализована уже в ранних версиях JDK 1.0.x. Sandbox предусматривает ограниченную среду для выполнения апплетов Java, неблагонадежных удаленных кодов. Суть принципа Sandbox состоит в том, что локальные коды считаются надежными, и в их распоряжение предоставляются файлы и другие системные ресурсы, а загружаемые удаленные коды - нет. Им открывается доступ только к определенным ресурсам в пределах Sandbox.

В рамках этой модели Java получает несколько дополнительных функций обеспечения безопасности, гарантирующих защищенность систем, допускающих коды внутрь. Каждый из компонентов должен размещаться в определенном месте и функционировать надлежащим образом, иначе не будет работать вся модель.

Так, например, средство проверки байт-кода должно гарантировать исполнение на клиенте только легитимного кода Java. Когда код достигает клиентской рабочей станции, верификатор проверяет каждый фрагмент на предмет соблюдения ограничений доступа и его целостности.

Еще один из компонентов защиты Java - это загрузчик классов, определяющий, при каких обстоятельствах апплету разрешено добавлять классы. Результаты компиляции исходного кода Java помещаются в файлы классов, содержащие самые разнообразные данные, например отладочную информацию или сведения о классе. Как правило, загрузчик классов поставляется вместе с браузером.

Есть и третий защитник - это диспетчер защиты Java, ограничивающий деятельность нелегитимного кода. Это средство допускает настройку и, помимо своих прочих многочисленных обязанностей, предусматривает, например, предотвращение установки новых загрузчиков классов, контроль над операциями с файлами, такими как чтение и запись, строгий

надзор за доступом к локальным файлам и контроль над созданием и доступом к системным программам и процессам.

Качество защиты Java зависит от того, насколько хорошо эти компоненты справляются с кодами, поступающими с удаленного сервера. Разумеется, любые недочеты могут сделать бесполезной всю эту стройную систему защиты, поэтому так важно быть в курсе изменений программного обеспечения современных браузеров.

В JDK 1.1.x компания впервые предложила возможность подписывать апплеты. Это означает, что-либо создатель кода, либо независимая компания, готовая поручиться за разработчика, проставляет на апплете цифровую подпись, которая служит дополнительной гарантией легитимности кода, поступающего с удаленного узла.

Цифровая подпись Java основана на технологии шифрования с открытым ключом. Принцип шифрования открытым ключом предполагает, что информация, зашифрованная одной стороной, может быть расшифрована второй стороной известным только ей личным ключом, связанным с первым некой математической функцией.

Почему мы так детально останавливаемся на этой технологии? Потому что данная технология имеет огромные потенциальные возможности по сравнению с любым другим языком программирования. Реализация операционной системы, написанной на Java, уже представлена и используется ведущими финансовыми и промышленными компаниями для коммерческого использования и управления коммерческой информацией.

Базы данных являются концентрацией информации как мелкой фирмы, так и крупного промышленного предприятия. Поэтому нельзя не сказать и о защите систем управления базами данных. Простейшая модель безопасности баз данных на самом элементарном уровне концепции обеспечения безопасности исключительно проста. Необходимо поддерживать два фундаментальных принципа: проверку полномочий и проверку подлинности (аутентификацию). Проверка полномочий основана на том, что каждому пользователю или процессу информационной системы соответствует набор действий, которые он может выполнять по отношению к определенным объектам базы данных. Проверка подлинности означает достоверное подтверждение того, что пользователь или процесс, пытающийся выполнить санкционированное действие, действительно тот, за кого он себя выдает.

К программным продуктам, разработанным для финансовых организаций, предъявляются высокие требования по безопасности и сохранности коммерческой информации. Для обеспечения безопасности требуется решить две программные задачи: во-первых, обеспечить безопасность системы с точки зрения несанкционированного доступа, во-вторых, проконтролировать неквалифицированные действия пользователей. Первая решается прежде всего правильным выбором технической платформы и опера-

ционной системы сервера базы данных, сетевого оснащения и СУБД. И хотя все это обеспечивает определенный уровень безопасности, в разработанной технологии должны быть предусмотрены дополнительные средства защиты, поддерживаемые самой прикладной системой. Для всех записей каждой таблицы базы данных рассчитывается контрольная сумма. При попытке изменить базу данных несанкционированным способом система должна диагностировать ошибку расчета контрольной суммы и выполнять какие-либо действия в зависимости от выбранной стратегии реакции на подобные ситуации. Контрольная сумма должна проверяться в стандартных функциях добавления и изменения. Кроме того, для контроля за правомочностью добавления и удаления информации из базы данных должны рассчитываться контрольные суммы для таблиц, выбранных администратором системы.

Неквалифицированные действия пользователей системы могут контролироваться протоколированием всех изменений, выполненных в БД прикладной системы. Это, естественно, снижает производительность системы, поэтому, как и для расчета контрольных сумм таблиц БД, администратор может ограничить список протоколируемых сущностей.

Существующие средства должны позволять финансовой организации - пользователю системы - самостоятельно определять стратегию безопасности приобретенной системы и полностью контролировать доступ к системе извне.

В свою очередь меры по организации безопасности в локальной сети должны предусматривать два аспекта. Безопасность в отношениях с внешним окружением и внутреннюю безопасность. Прежде всего необходимо убедиться в том, что сеть функционирует надежно, именно недостаточный уровень настройки сети зачастую является основанием для "нападений". Далее необходимо соблюдать определенные меры, которые определяют задачи системного администратора в области безопасности работы:

1. Создать на сервере необходимые учетные записи пользователей и задать их права и пароли. Для временных учетных записей установить срок действия. Чтобы защитить своих пользователей и ресурсы, менять пароли и сроки действия чаще. Если возможно, использовать наиболее строгие методы аутентификации (например, установление паролей с фиксированным количеством попыток набора и регистрацией количества входа).

2. Определить максимально возможное и в то же время достаточно необходимое количество правил обеспечения безопасности. Создать резервные копии данных системы и хранить их вне узла. Периодически проводить проверку сети на наличие возможных проблем, нарушений системы безопасности и вирусов. Использовать средства регистрации и контроля операционной системы для обнаружения проблем на их начальной стадии.

3. Перед отправкой по Internet кодировать все материалы, предназначенные для конфиденциального использования.

4. Организовать для своего персонала занятия по безопасности и обеспечить выполнение ими соответствующих правил.

Роль руководителя отдела, организации - не только управление по созданию хорошо структурированной "прозрачной" информационной структуры, позволяющей практически любому пользователю распознать логически правильно построенную, информативно грамотную иерархию базы данных организации, но и преднамеренный контроль, позволяющий, опираясь на описанную выше структуру, надежно, быстро и эффективно управлять системой.

При организации взаимодействия руководителя организации и системного администратора необходимо прежде всего учитывать ту обязательную информацию, которой должен обладать руководитель для обеспечения своевременного и беспрепятственного использования информационной базы данных организации. Прежде всего, руководитель должен иметь наивысшие права доступа в инфосистему организации, а это права администратора. К тому же в некоторых случаях является эффективным локализация наиболее существенной для руководителя информации, т.е. независимость ее использовании от сетевых ресурсов. Поэтому очень важным и принципиальным является необходимость обеспечения как контролируемого списка пользователей, так и механизмов замещения администраторских функций.

В результате такого подхода к организации работы сети повышается роль руководителя. Он должен обеспечить техническую и организационную деятельность, а также контроль за организацией информационной структуры.

Что является принципиально важным сегодня, так это необходимость детально структурировать информационную систему и определить спектр возможных решений по безопасности, детально изучить самые необходимые в ней элементы и принять решение.

СОВРЕМЕННЫЕ ПРИНЦИПЫ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ ЗАПАСАМИ НА ПРЕДПРИЯТИЯХ

ISBN 966-7418-41-3

Бондарева И. А., аспирант каф. экономики предприятия

Обобщен опыт применения методов управления производственными запасами на промышленных предприятиях. Сформулированы современные