УДК 681.3 (575.2)

Г.А.ТОКТОГУЛОВА, А.А.ТОРОЕВ, Г.А.ЭСЕНАЛИЕВА

E-mail: ksucta@elcat.kg.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Бул макала компьютердик тутумдарда жана тармактарда маалыматты коргоодо кыскача талдоо жана заманбап ыкмалары, каражаттары, технологиялары каралып чыкканга арналган.

Данная статья посвящена краткому анализу и рассмотрению современных методов, средств, и технологий защиты информации в компьютерных системах и сетях.

Given article is devoted the short analysis and consideration of modern methods, means, and technologies of protection of the information in computer systems and networks.

Кто владеет информацией – тот правит миром.

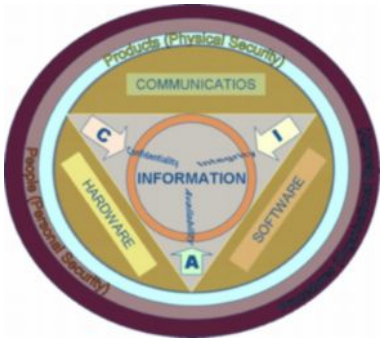
Руперт Мердок

Быстрый рост глобальной сети Интернет и стремительное развитие информационных технологий привели к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. Новые технологические возможности облегчают распространение информации, повышают эффективность производственных процессов. Однако, несмотря на интенсивное развитие компьютерных средств и информационных технологий, уязвимость современных информационных систем и компьютерных сетей, к сожалению, не уменьшается. Поэтому проблемы обеспечения информационной безопасности привлекают пристальное внимание как специалистов в области компьютерных систем и сетей, так и многочисленных пользователей.

Без знания и квалифицированного применения современных технологий, стандартов, протоколов и средств защиты информации невозможно достигнуть требуемого уровня информационной безопасности компьютерных систем и сетей.

Проблемы информационной безопасности. *Применение информационных технологий (ИТ) требует повышенного внимания к вопросам информационной безопасности. Разрушение информационного ресурса, его временная недоступность или несанкционированное использование могут нанести компании значительный материальный ущерб. Без должной степени защиты информации внедрение ИТ может оказаться экономически невыгодным в результате значительных потерь конфиденциальных данных, хранящихся и обрабатываемых в компьютерных сетях /3/.*

Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода. Целью информационной безопасности является обезопасить ценности системы, защитить и гарантировать точность и целостность информации и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, к ней обеспечивается доступ или она распространяется /1/.



Классически считалось, что обеспечение безопасности информации складывается из трех составляющих: конфиденциальности, целостности, доступности. Точками приложения процесса защиты информации к информационной системе являются аппаратное обеспечение, программное обеспечение и обеспечение связи (коммуникации). Сами процедуры (механизмы) защиты разделяются на защиту физического уровня, защиту персонала и организационный уровень.

Конфиденциальность – защита конфиденциальной информации от несанкционированного раскрытия или перехвата.

Целостность – обеспечение точности и полноты информации и компьютерных программ.

Доступность – обеспечение доступности информации и жизненно важных сервисов для пользователей, когда это требуется.

Информация существует в различных формах. Ее можно хранить на компьютерах, передавать по вычислительным сетям, распечатывать или записывать на бумаге, а также озвучивать в разговорах. С точки зрения безопасности все виды информации, включая бумажную документацию, базы данных, пленки, микрофильмы, модели, магнитные ленты, дискеты, разговоры и другие способы, используемые для передачи знаний и идей, требуют надлежащей защиты.

Так как же все-таки защищать информационные системы? Существует довольно много каналов утечки информации. По физическим признакам их можно разделить на следующие группы: акустические (включая вибрационные и акустопреобразовательные), визуально-оптические (наблюдение, фотографирование), электромагнитные (в том числе магнитные, электрические и параметрические), материально-вещественные (бумага, фото, магнитные носители, отходы), компьютерный метод съема (вирусы, закладки, логические бомбы), перехват при передаче по каналам связи.

Часть задач обеспечения безопасности можно решить при помощи физических средств защиты: надежные серверные, несгораемые шкафы, средства ограничения доступа в помещения, контроль за использованием устройств хранения и ввода/вывода информации (магнитные и

оптические накопители, порты ввода/вывода на компьютерном и коммуникационном оборудовании), за печатающей и копировальной техникой, пожарная и охранная сигнализация, средства видеонаблюдения.

Из всего этого многообразия рассмотрим подробно способы защиты от компьютерного метода съема и от перехвата при передаче по каналам связи. Если говорить о технических средствах защиты, то их целесообразно разбить на несколько групп в зависимости от точки приложения: средства защиты периметра сети, обеспечение безопасных соединений и обеспечение безопасности в локальных и беспроводных сетях.

Защита периметра

Для защиты периметра сети применяются устройства, называемые межсетевыми экранами. Существует несколько поколений таких устройств. *Первое* – экраны с пакетной фильтрацией (Packet Filtering Gateways), которые работают на сетевом и транспортном уровне модели OSI и, как правило, анализируют следующие поля пакетов: IP-адрес источника и назначения, номер протокола, порт (TCP, UDP) источника и назначения. Они имеют хорошую масштабируемость и производительность, но обеспечивают не очень высокий уровень безопасности. На сегодняшний день практически все маршрутизаторы и большинство коммутаторов третьего уровня обладают функциональными возможностями экранов с пакетной фильтрацией.

Второе поколение – экраны уровня соединения (Circuit Level Gateways) /1/. Эти устройства работают на сетевом, транспортном и сеансовом уровнях и анализируют большое число полей: IP-адрес источника и назначения, номер протокола, порт (TCP, UDP) источника и назначения, информацию о последовательности и состоянии соединения (устанавливается, установлено, завершается), т.е. флаги пакетов. Главное их отличие от предыдущих в том, что экраны уровня соединения ведут так называемую таблицу соединений (session state table), в которую заносят информацию об установленных сессиях и удаляют ее из таблицы только при их завершении. Благодаря такому алгоритму работы обеспечивается гораздо более высокий уровень безопасности – устройства оперируют не только информацией, содержащейся в анализируемом пакете, а и «знают», что происходило раньше. Такие экраны, например, позволяют запретить установку соединения со стороны публичных сетей в сторону локальных и создать динамические правила для прохождения пакетов из Интернета в локальную сеть, если сессия была инициирована именно из нее. С их помощью можно защититься от некоторых атак, использующих подмену адресов, и атак типа «отказ в обслуживании» (Denial of Service – DoS). Производительность экранов уровня соединения практически такая же, как и устройств с пакетной фильтрацией.

Третье поколение – экраны уровня приложений (Application Level Gateways), которые могут отслеживать корректность работы протоколов данного уровня, например, блокировать определенные команды, терминировать сессию в случае неправильного порядка команд. Для протоколов, использующих динамические порты (FTP, SIP, H.323), устройства могут создавать динамические правила для открытия соответствующих портов. Они могут блокировать загрузку определенных файлов или типов файлов, ограничивать доступ к определенным Web-ресурсам,

блокировать Java, апплеты ActiveX, Cookies. Экраны уровня приложений, как правило, не выпускаются в виде самостоятельных устройств или отдельного ПО, а являются службами в межсетевых экранах с полной пакетной проверкой (Statefull Packet Inspections – SPI).

Экраны с полной пакетной проверкой дают возможность анализировать пакеты на всех уровнях модели OSI. К этому типу относится большинство выпускаемых сегодня устройств, однако это не означает, что они могут анализировать все протоколы уровня приложений. Самые дешевые из них умеют работать только с протоколом HTTP, более продвинутые поддерживают большее количество протоколов (как правило, еще и FTP, SMTP, POP3, IMAP4). Наиболее функциональные модели могут работать с VoIP-протоколами (такими как SIP, H.323, MGCP, SCCP) и некоторыми другими протоколами уровня приложений. Поэтому при выборе устройств не следует особо обращать внимание на термин SPI, так как он практически ни о чем не говорит. Необходимо детализировать характеристики устройств, перечень поддерживаемых функций, технологий и протоколов, а также такой немаловажный параметр, как производительность.

Рис. 1. Прозрачные межсетевые экраны инспектируют сессии, установленные между внешними и внутренними хостами

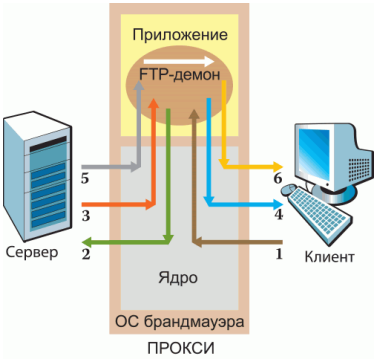


Рис. 2. Межсетевые экраны-посредники устанавливают сессию с хостом-источником, а потом от его имени – сессию к хосту назначения

Экраны уровня соединения и уровня приложения бывают двух типов: прозрачные (transparent) и посредники (proxy). Прозрачные межсетевые экраны инспектируют сессии, установленные между внешними и внутренними хостами (рис. 1). Межсетевые экраны-посредники устанавливают сессию с хостом-источником, а потом от его имени – сессию к хосту

назначения (рис. 2). Такие устройства обеспечивают более высокий уровень безопасности, поскольку усложняется реализация атаки, т.е. атакуется сразу не конечный хост, а брандмауэр-посредник. Однако их недостаток – невысокое быстродействие.

Имеются как программные, так и аппаратные реализации межсетевых экранов. Первые представляют собой программное обеспечение (ПО), функционирующее на универсальной аппаратной платформе (обычные серверы или ПК) поверх открытой операционной системы. Какой экран выбрать, программный или аппаратный? При разработке программных решений существует меньше различных технологических ограничений, к этому процессу привлекается, как правило, меньшее количество разработчиков, и, соответственно, их стоимость зачастую ниже. То же самое справедливо и для межсетевых экранов – программные реализации по сравнению с аналогичными по функциональным возможностям аппаратными ощутимо дешевле.

Споры о предпочтительности программных или аппаратных решений ведутся давно, но любые технические средства – это лишь инструмент в руках тех, кто их эксплуатирует. И чаще всего проблемы с безопасностью возникают из-за невнимательности или низкой квалификации ответственных за это лиц, а не выбора той или иной платформы. Опытный сетевой администратор может из программного экрана сделать решение не хуже, а то и лучше, чем аппаратное. Вопрос в том, что таких специалистов не так уж много. Мало того, некоторые из известных производителей аппаратных межсетевых экранов используют в своих устройствах программные решения других компаний. В данном случае производитель аппаратного решения как раз и берет на себя те проблемы, которые присущи программным продуктам, т.е. подбирает специализированную аппаратную платформу, устанавливает и конфигурирует ОС и ПО межсетевого экрана. В качестве примера можно привести устройства от Nokia и Nortel Networks, в которых используются программные продукты компании Check Point. Аппаратные экраны конструктивно могут быть реализованы в виде отдельного устройства, а также как модуль или программная служба маршрутизатора или коммутатора.

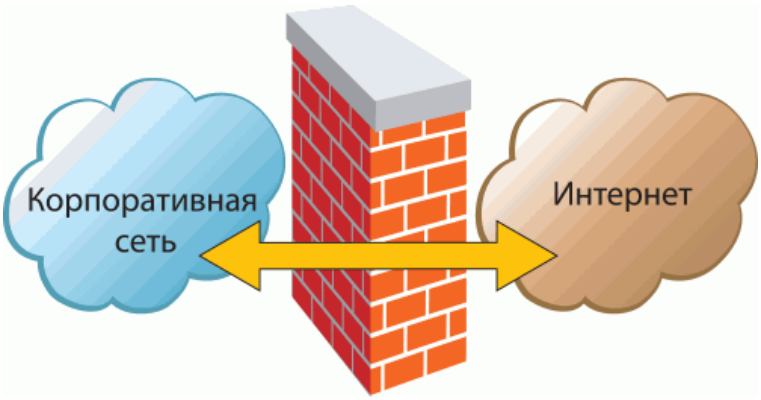


Рис. 3. В простейшем случае межсетевой экран устанавливается между корпоративной и публичной сетями и контролирует проходящий через него трафик

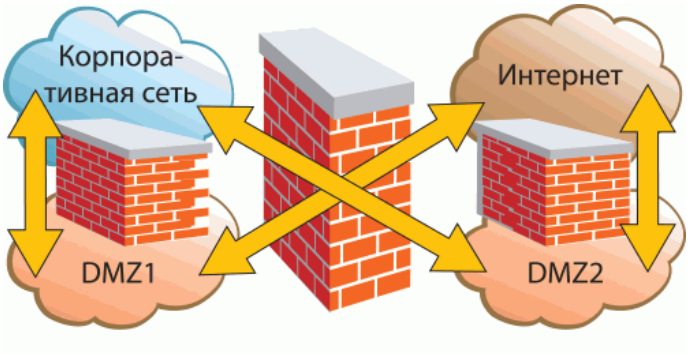


Рис. 4. При установке двух межсетевых экранов между ними выделяется так называемая демилитаризованная зона (DMZ)

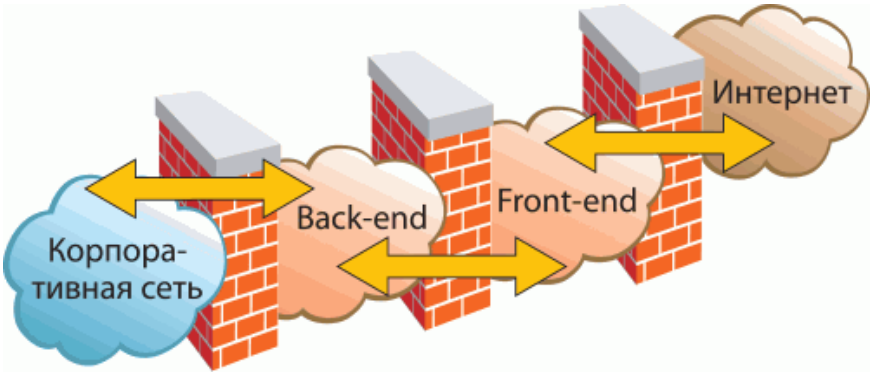


Рис. 5. Демилитаризованных зон может быть несколько

Итак, межсетевые экраны предназначены для защиты периметра сети и, соответственно, должны устанавливаться на ее границе таким образом, чтобы весь трафик, циркулирующий между сетями, проходил через них. Существует довольно много различных топологий установки устройств, рассмотрим лишь основные. Простейший из них представлен на рис. 3: экран располагается между корпоративной и публичной сетями и контролирует проходящий через него трафик. Еще один вариант – установка двух межсетевых экранов и выделение между ними так называемой демилитаризованной зоны (DMZ, рис. 4). Таких зон может быть несколько (рис. 5).

Как правило, для организации демилитаризованных зон используют не несколько устройств, а реализуют их на одном, применяя для каждой различные физические или логические интерфейсы экрана. Предпочтительнее именно физические интерфейсы – в этом случае трафик из разных зон не будет проходить по одним и тем же физическим линиям связи.

DMZ – это зона с пониженным уровнем доверия, т.е. кроме нее обязательно есть еще две: зона внутренней локальной сети (с самым высоким уровнем доверия) и зона внешней публичной сети (с самым низким уровнем доверия) /2/.

При правильной реализации межсетевой экран может обеспечить довольно высокий уровень безопасности, однако следует помнить, что данные устройства не защищают от вирусов и «троянских» программ. Межсетевые экраны, даже работающие на уровне приложений, не просматривают содержимое пакета (поле данных), они анализируют только служебные поля. И если сессия HTTP, FTP, SMTP или другого протокола уровня приложений протекает нормально, то она не будет заблокирована, но в полях данных пакетов, передаваемых в пределах этих сессий,

может находиться вредоносное содержимое. Поскольку межсетевой экран устанавливается на периметре, он не защищает и от атак, реализованных из локальной сети. Для защиты от вышеперечисленных угроз применяются устройства, называемые системами обнаружения вторжений (Intrusion Detection System – IDS).

Тема информационной безопасности настолько широка, что полностью осветить ее невозможно. Описанные подходы и механизмы обеспечения безопасности оказываются наиболее эффективными для обеспечения информационной безопасности информационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Шаньгин В. Компьютерная безопасность информационных систем. – СПб.: Питер, 2008.
2. Яремчук С. Защита вашего компьютера. – СПб.: Питер, 2008.
3. www.npp-itb.spb.ru