CIO
Chief Information Officer
РУКОВОДИТЕЛЬ ИНФОРМАЦИОННОЙ СЛУЖБЫ • ИЮНЬ 2002 • № 5 (5)

Критерии выбора средств защиты информации

Илья Трифаленков, Владимир Макоев

Рынок средств защиты информации динамично развивается, формируя, с одной стороны, потребности во всех сложных решениях, с другой — разнообразные предложения производителей. Цена вопроса составляет, как правило, около десяти процентов от общих затрат на построение и эксплуатацию информационных систем. При том, что стоимость систем состовляет не редко миллионы, а подчас и десятки миллионов долларов, получается весьма солидная цифра.

Наиболее надежный способ понять, почему защита информационных ресурсов стоит именно столько, от каких угроз она способна защитить и от каких не способна, при каких условиях предложенные средства защиты будут работать — это провести комплексное проектирование подсистемы информационной безопасноста, а после ее внедрения аттестовать систему и убедиться в адекватности предложенных средств. К сожалению, в наших усповиях очень часто развитие системы происходит хаотически. При этом важную роль играет уверенность в правильности применяемых частных решений по защите информации, как с точки зрения непосредственно возложенных на них задач, так и с точки зрения их соответствия ближайшим и более отдаленным перспективам развития ИС.

Рассмотрим, какие критерии могут быть предложены для различных классов средств защиты информации и что таится за заявлениями различных производителей ПО.

При выборе средств защиты (как, впрочем, и других решений в области информационных технологий) пользователь в первую очередь сталкивается с каскадом маркетинговых заявлений поставщиков того или иного решения. Некоторые рассказывают об «уникальной технологии, обеспечивающей комплексную защиту информации», другие предложат «бесплатный» проект для своего решения, а третьи объяснят в своем учебном центре, как правильно выбрать их систему защиты информационных ресурсов. Если дело происходит в России, то практически каждый скажет, что его система «сертифицирована ФАПСИ (Гостехкомиссией)» либо что «для продуктов этого класса сертификация не требуется».

Рынок ИТ, вследствие высочайших темпов его развития, действительно находится под мощным воздействием маркетинговых механизмов, которые способны дать искаженное

представление о свойствах продукта и критериях выбора, и давлению которых трудно противостоять. Трудно, однако, не означает — невозможно. Дело в том, что хотя маркетинг и дает искаженную картину, под ней скрываются вполне реальные свойства и характеристики решений. Если при этом еще и понимать причины, искажающие картину в ту или иную сторону, то ока-жется, что из маркетинговых и рекламных материалов можно извлечь гораздо больше информации, чем там на первый взгляд содержится, и, как правило, больше, чем хотели бы сообщить авторы рекламы.

Для того чтобы выяснить, какие средства защиты применимы для конкретной ИС, необходимо сформулировать требования к ним. Основой такого определения должна быть следующая позиция: все средства защиты всего-навсего предоставляют собой инструментарий для реализации политики безопасности — набор управленческих решений, направленных на защиту информации, и установленных на их основе правил работы пользователей и администраторов ИС.

Поэтому основные вопросы при выборе того или иного средства защиты информации должны звучать приблизительно так:

• для чего будет применяться средство?

• от каких угроз это средство будет ограждать и в какой степени?

• какие правила работы с информационными ресурсами будут (могут быть) реализованы?

Отсутствие внятных ответов на указанные вопросы означает неготовность организации к эффективному использованию приобретаемых средств защиты.

Рассмотрим, какие требования могут и должны быть выдвинуты к различным средствам защиты информации: межсетевым экранам, средствам создания виртуальных частных сетей (VPN), средствам контекстного анализа информации.

ОСНОВНЫЕ КРИТЕРИИ ВЫБОРА СРЕДСТВ VPN

Вопросы производительности также значимы при выборе VPN-решения. При этом стоит отдавать себе отчет, что целью является обеспечение заданного качества сервисов в данной СПД, и осторожно относиться к изобретаемым некоторыми производителями количественным характеристикам, которые для их решения лучше, чем у конкурентов, и которые якобы отражают эффективность применения VPN. Единственный надежный показатель сегодня — это реальные сравнительные испытания систем. В таких испытаниях необходимо, во-первых, полностью моделировать среду передачи данных и реальные скорости,реализуемые в сети передачи данных. В каналах Ethernet 100 Мбит и FrameRelay 64 Кбит, например, эффективность работы решений будет определяться принципиально разными факторами, поэтому испытания в условиях простого стенда из четырех машин,соединенных технологиями локальной сети, практически ничего не говорят о том, как все это будет работать «на самом деле». Во-вторых, необходимо учитывать специфику «коллективных эффектов», проявляющихся в том, что если система из двух узлов показывает прекрасные результаты на испытаниях, из этого совсем не следует, что такая же система из сотни узлов вообще будет работать. Наконец, в-третьих, существенным оказывается моделирование реальной структуры информационных сервисов, а не запуск тестовых утилит, в противном случае результаты испытаний также могут оказаться неадекватными. Сегодня VPN обычно используется не только для защиты передачи данных, но и для мультимедийных сервисов, реализованных на той же инфраструктуре (IP-телефония, видеоконференции). Чтобы применение VPN не приводило к потере качества сервисов, решения должны обеспечивать приоритизацию в передаваемой информации.

Если предполагается часть информационных потоков направлять во внешнее информационное пространство (без шифрования), необходимо убедиться, что шлюз VPN умеет это делать. Иначе придется организовывать доступ к этим ресурсам в обход средств защиты, что само по себе создает дополнительные угрозы информационным ресурсам. С точки зрения сертификации существенно, что многие средства VPN сертифицированы сегодня как межсетевые экраны, что не дает возможности легального использования собственно свойств VPN. Это еще одна иллюстрация необходимости внимательно изучать представляемые производителем сертификаты.

Функционалыные требования

К средствам защиты информации обычно предъявляется две группы требований: функциональные требования, описывающие механизмы безопасности, которые должно реализовывать то или иное средство, и требования гарантий, описывающие механизмы,

гарантирующие, что функциональные требования будут выполнены корректно и что средство защиты не будет обладать недокументированными возможностями, в том или ином случае препятствующими его работе.

Основные критерии выбора межсетевого экрана

Требования гарантированности обычно подтверждаются сертификатом Гостехкомиссии на соответствие руководящему документу «Защита информации. Проверка на отсутствие недекларированных возможностей»; сертификат должен выдаваться не на отдельные экземпляры и партии продуктов, а на их производство. Крайне желательно, чтобы такие сертификаты были, независимо от того, о каком виде средств защиты информации идет речь.

Межсетевые экраны

Межсетевые экраны (МЭ) уже много лет входят в обязательную номенклатуру средств защиты. Изобилие решений в этой области (только коммерческих МЭ сущесгвует более 150) ставит вопрос о требованиях и критериях выбора довольно остро. Естественно, что высокая конкуренция приводит к стремлению производителей навязать потенциальному пользователю свою «систему ценностей».

Основных критериев для выбора межсетевого экрана, на наш взгляд, три: глубина проводимого анализа информационного обмена, собственная защищенность экрана и соответствие требованиям по производительности.

Глубина проводимого анализа определяется степенью раскрытия информации, передаваемой в процессе информационного обмена. В минимальном случае это фильтрация на сетевом уровне, в более спожных системах это фильтрация с виртуальным соединением; наиболее детальный анализ производят экраны, работающие на прикладном уровне. Именно они обеспечивают наибольшую защищенность и могут в большинстве случаев быть рекомендованы для установки. Экраны с меньшими возможностями анализа информации оказываются эффективны, когда устанавливаются у провайдера информационных услуг, который не может в полной мере определять политику безопасности своих клиентов, но должен обеспечивать получение ими информационных сервисов. Заметим, что в этом случае есть серьезный риск потерять контроль над реальной структурой информационного обмена, так как без применения шлюзов приложений тип приложения определяется формально, по номеру порта в IP-пакете, что предоставляет злоумышленнику потенциальную возможность пользоваться недозволенным сервисом, выдавая его за разрешенный.

При анализе собственной защищенности критична принципиальная невозможность перехода системы в состояние «открытости защищаемой сети для всех». Полностью исключить такую ситуацию могут опять-таки только шлюзы приложений, где пакеты каждый раз пересобираются заново. Это, кстати, исключает попадание в локальную сеть пакетов с некорректными полями или опасными опциями.

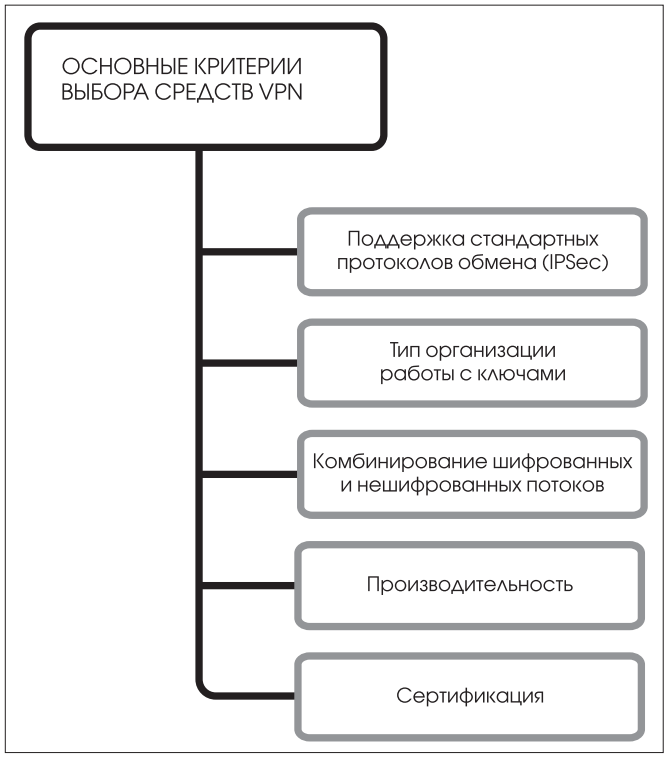
Немаловажным является соответствие требованиям по производительности. Поскольку не существует общепризнанной методики измерения характеристик производительности экранов, стоит порекомендовать проведение испытаний на реально существующей структуре информационного обмена. Следует обратить также внимание на устойчивость к пиковым нагрузкам, которая традиционно высока для UNIX-систем либо аппаратных решений.

Многие межсетевые экраны сегодня сертифицированы на соответствие РД Гостехкомиссии России. Однако чтобы сертификаты были применимы, необходимо внимательное сопоставление сертификата и условий предполагаемого использования экрана.

Виртуальные частные сети

Средства VPN (виртуальные частные, или защищенные сети) обеспечивают защищенность передаваемой информации при использовании общедоступных сетей передачи данных. В настоящий момент количество решений, обеспечивающих построение VPN, также достаточно велико, поэтому вопрос критериев выбо-ра весьма актуален.

Один из ключевых факторов для средств VPN — реализованный в них протокол защищенного информационного обмена. Сегодня бесспорным стандартом является IPSec, и поддержка именно этого протокола является обязательным требованием. Напротив, использование нестандартных протоколов чревато, с одной стороны, недостаточно продуманной логикой («изобретенные» протоколы редко подвергаются даже функционалыному тестированию, не говоря уже об использовании формальных методов анализа), с другой стороны, есть проблема совместимости с сетевым оборудованием, которой для нестандартных протоколов никто не гарантирует. Кроме того, в результате использования такого решения возникает зависимость от поставщика — никто другой не знает «устройства» закрытых решений.



Вторым определяющим фактором в выборе VPN является организация работы с ключевой информацией. В решении обязательно должно использоваться динамическое распределение ключей с центром (центрами) их распределения, что позволяет администрировать распределенную систему кодирующих (или шифрующих) шлюзов централизовано. Сюда же примыкают вопросы возможности динамического изменения конфигурации, введения в систему новых узлов и отключения старых.

Если добавление в систему нового узла требует переконфигурирования всех остальных, масштабирование системы свыше 5 узлов на практике становится нереальным.

Основные критерии выбора средств контекстного анализа

К средствам контекстного анализа принадлежат системы, осуществляющие мониторинг и фильтрацию почтового трафика. Рынок этих систем сравнительно молодой, однако в настоящее время решения с применением технологии контекстного анализа пользуются большой популярностью.

Какие критерии выбора данных средств являются, на наш взгляд, наиболее значимыми?

В первую очередь, это глубина проводимых проверок, то есть количество и разнообразие критериев анализа электронной почты. При этом болыuое значение имеет способность осуществлять фильтрацию по любым атрибутам сообщений, по объему сообщений и вложенных файлов, по количесrву и типу вложений, по глубине вложенности, возможность анализа содержимого прикрепленных файлов, вне зависимости от того, являются ли эти файлы сжатыми или архивными. Существенным преимуществом многих продуктов является способность создания собственного сценария

обработки сообщений электронной почты. Во-вторых, наиболее важным критерием оценки средств контекстного анализа является мощность и гибкость системы реагирования по результатам анализа содержимого электронной почты. В данном случае при оценке необходимо учитывать разнообразие вариантов действий, осуществляемых по результатам проверок.

В-третьих, в последнее время большое значение для обеспечения информационной безопасности приобрело наличие в компании архива почтовых сообщений. Некоторые разработчики систем контекстного анализа предусматривают прикрепление к своим продуктам специальных модулей архивирования. Именно наличие архива электронной почты и определяет в настоящее время полнофункциональность таких систем. При этом ведение архива — это не просто автоматическая архивация почтовых сообщений в файл, а способность регистрации сообщений и учета необходимой информации на протяжении всего жизненного цикла сообщения, возможность получения любых выборок и статистики из архива по создаваемым запросам на основании любых критериев.

В-четвертых, отличительным признаком средств контекстного анализа является способность получения отчетов и статистики. Многие продукты имеют в своем арсенале только встроенные виды отчетов, другие могут осуществлять лишь просмотр статистики работы конкретного пользователя системы электронной почты.

На наш взгляд, наиболее совершенными являются системы, которые способны обеспечить получение любых выборок и статистики из архива по создаваемым запросам, создание специфических запросов на SQL, генерацию любых видов отчетов для анализа эффективности использования почтового сервиса компании.

В-пятых, одним из основных критериев оценки систем контекстного анализа должна быть поддержка продуктом кодировок кириллицы (Win-1251, DOS-866, ISO-8859.5, KOI-8, MAC, cp866), что дает возможность анализа русско-язычных текстов. Большинство продуктов иностранного производства не способны обеспечить поддержку кодировок кириллицы, а это в значительной степени снижает возможность их использования на территории РФ.

В-шестых, большое значение имеет удобство администрирования системы, что предполагает наличие русскоязычного интерфейса, возможность разделения функций управления и администрирования системы, то есть разграничения доступа различных категорий пользователей к средствам управления системой.

И, наконец, необходимо сказать о важности сертификации данных средств Гостехкомиссией РФ. При проведении испытаний того или иного продукта Гостехкомисия подтверждает его соответствие определенным техническим условиям, а это является подтверждением качества данного продукта. Кроме того, сертификация предоставляет возможность использования продукта государственными структурами, где наличие сертификата обязательно.

Общесистемные средства

Для решения проблем раз-граничения доступа на уровне операционных систем и СУБД используется та или иная мо-дель доступа к информацион-ным ресурсам. Хотя набор таких моделей достаточно широк, только относительно небольшое число реализовано в конкретных продуктах либо может быть туда встроено без значительной модификации

исходного продукта.

Наиболее распространенные модели доступа на сегодняшний день основаны на разработках «Оранжевой книги» — первого широко распространенного стандарта в области безопасности информационных систем. Предложенная в этой работе классификация использовала две модели доступа к ресурсам — модель произвольного управления доступом (DAC, классы C1-C2) и модель принудительного управления доступом (MAC, классы B1-B3). Отечественная нормативная база, в целом построенная на тех же принципах, что и «0ранжевая книга», предлагает модель DAC для систем, не содержащих сведений, составляющих государственную тайну (классы АС 1Д-1Г), и модель MAC для прочих систем (классы АС 1В-1А).

Именно в соответствии с моделью DAC построены большинство составляющих КИС, начиная с операционных систем и кончая СУБД. Причина такой распространенности кроется в простоте реализации указанной модели в сочетании с возможностью реализовать достаточно широкий спектр управленческих решений, принятых в рамках той или иной организации.

Заключение

Очень важно понимание заказчиком задач, которые должно решать то или иное средство защиты, изучение основных характеристик и результатов сравнительных испытаний.

На современном этапе наиболее распространены такие средства защиты информации, как межсетевые экраны, средства VPN, средства контекстного анализа и общесистемные средства.

Таким образом, можно сказать, что при получении информационных и маркетинговых материалов от разработчиков или поставщиков необходимо, в первую очередь, выявить базу критериев, по которым оценивается то или иное средство защиты. Эти критерии можно разделить на два типа: общие критерии для средств защиты информации, такие как собственная защищенность, производительность, сертификация, стоимость, и функциональные критерии, зависящие от каждого конкретного средства.

Отсутствие в информационных и рекламных материалах основных критериев или ввод лишних, незначительных позволяет судить об истинных качествах предлагаемого средства и достоверности маркетинговых заявлений.