Вихорев С.В.

Березин А.С.

Новые подходы к проектированию систем защиты информации

За последние два десятилетия лет обеспечение информационной безопасности (ИБ) корпоративных информационных систем (ИС) выросла из частной проблемы отдельных компаний в большое самостоятельное направление развития современных информационных технологий. Наглядным подтверждением этому стало появление специализированных международных институтов, занимающихся проблемами защиты информации; открытых стандартов на технологии обеспечения ИБ; законодательной базы, регулирующей вопросы построения систем защиты информации (СЗИ); специализированных продуктов и решений по защите информации и т.д. Но главное – за это время появился реальный растущий рынок разнообразных продуктов и услуг в области обеспечения ИБ корпоративных ИС.

Можно выделить четыре основных типа или, скорее, этапа развития СЗИ:

- *однокомпонентные СЗИ*, которые строятся на базе одного, как правило, узкоспециализированного продукта по защите информации (в большинстве случаев таким продуктом становился антивирусный пакет);
- *многокомпонентные СЗИ*, строящиеся уже на базе нескольких продуктов, каждый из которых решает свою конкретную задачу. При этом используемые в многокомпонентной СЗИ продукты и технологии по защите информации никак не связанны между собой ни на техническом, ни на организационном уровнях;
- *комплексные СЗИ* – дальнейшее развитие многокомпонентных СЗИ, в которых используемые продукты, технологии и решения объединяются в единую систему на организационном уровне с тем, чтобы обеспечить максимальную степень защищенности всей КИС в целом. Очевидно, что при этом стойкость всей СЗИ эквивалентна стойкости самого «слабого» ее звена;
- *интегрированные СЗИ*, в которых все элементы комплексных СЗИ объединяются (вернее интегрируются) не только на организационном, но и на техническом, и даже технологическом уровнях. В такой интегрированной системе компрометация одного из элементов защиты должна надежно компенсироваться противодействием других ее элементов.

К сожалению, на современном этапе развития технологий обеспечения ИБ использование явления синергизма в масштабах всей корпоративной СЗИ пока еще невозможно в силу отсутствия на рынке реальных решений, позволяющих строить именно интегрированные СЗИ. По-видимому, это объясняется недостаточной зрелостью международных стандартов в области защиты информации, хотя движение в этом направлении прослеживается уже достаточно явно. С другой стороны построение многокомпонентных, а тем более однокомпонентных СЗИ в большинстве случаев уже не является современным решением проблемы ИБ, особенно для крупных компаний. Поэтому, на наш взгляд, в настоящее время оптимальным решением является построение именно комплексных СЗИ (КСЗИ).

Как показывает практика, проектирование комплексной (в широком смысле этого слова) СЗИ является достаточно сложной системно-аналитической задачей, которая требует специальной и достаточно строгой методики. К сожалению, предлагаемые известными российскими и международными институтами методики (Гостехкомиссия России, ISO, ICSA, CSI и др.) в большинстве своем носят слишком общий и отчасти даже «философский» характер, что не позволяет использовать их как реальный инструмент работы системного интегратора, работающего в жестких рыночных условиях.

В данной статье сделана попытка обобщить собственный опыт московской компании ЭЛВИС+ (www.elvis.ru), системного интегратора в области ИБ, по проектированию КСЗИ для ряда крупных корпоративных заказчиков. Предлагаемая методика носит открытый характер и, по нашему мнению, может быть полезна компаниям-системным интеграторам для более четкого структурирования своего подхода к проектированию КСЗИ, а компаниям-заказчикам – в качестве инструмента выработки технических требований и контроля корректности построения необходимой им системы защиты.

Известно, что в области IT давно и достаточно успешно применяется стековая модель описания сложных ИС, в которой система рассматривается в виде иерархии нескольких функционально-единообразных уровней. Поскольку любая СЗИ в конечном итоге должна «накладываться» на реальную ИС, для ее описания также целесообразно было бы использовать многоуровневую иерархическую модель. Это позволило бы, с одной стороны, четко определить основные задачи, решаемые в рамках СЗИ, а также систему связей между этими задачами и, с другой стороны, корректно описать порядок взаимодействия двух различных СЗИ. На наш взгляд типовую СЗИ можно рассмотреть в виде следующих пяти функциональных уровней:

1) Физический уровень: физическая охрана помещений, в которых обрабатывается или хранится конфиденциальная информация; организация контроля доступа сотрудников в данные помещения; ответственное хранение резервных (архивных) копий конфиденциальных информационных ресурсов; обеспечение энерго- и пожаробезопасности всей ИС в целом и др.

2) Технологический уровень: устранение угроз безопасности информации, связанных с использованием некачественных аппаратно-технических средств обработки и хранения информации и систем передачи данных; контроль качества (в т.ч. целостности) используемого программного обеспечения; организация резервных хранилищ данных, кластеров; периодическое архивирование данных; контроль лицензионной политики; организация защиты от вредоносных и разрушающих программ и т.д.

3) Пользовательский уровень: устранение угроз, связанных с некорректными (случайными, ошибочными и т.д.) действиями персонала или умышленными действиями нелояльных сотрудников компании или третьих лиц (разграничение доступа к информационным ресурсам, защита от НСД, аутентификация пользователей, включая удаленных и мобильных сотрудников компании и т.д.).

4) Сетевой уровень: система защиты на этом уровне должна устранить угрозы, исходящие от злоумышленников, находящихся как внутри, так и вне пределов защищаемой КИС на уровне базовой сетевой инфраструктуры (сегментация ЛВС по уровням конфиденциальности обрабатываемой информации, защита информации при ее передаче по внешним и внутренним каналам связи, защита от внешних вторжений и т.д.)

5) Уровень управления: организация связи с системой управления ИС (если таковая есть); управление, координация и контроль осуществляемых организационных и технических мероприятий на всех низлежащих уровнях СЗИ; контроль полноты реализации функций защиты на каждом из уровней и неразрывности функционирования СЗИ при переходе от уровня к уровню; окончательный (а далее периодический) контроль стойкости и комплексности всей СЗИ в целом (например, путем применения специальных технических средств «дружественного взлома») и т.д.

Следует сказать, что в конкретной автоматизированной системе наличие всех пяти уровней СЗИ в явном виде не всегда обязательно, хотя стойкость системы защиты напрямую зависит от наличия каждого уровня и его функциональной наполненности. Очевидно также, что стоимость и сложность реализации СЗИ существенным образом растет от уровня к уровню, причем снизу-вверх. Так, например, значительную часть необходимых функций СЗИ на физическом уровне можно реализовать простыми и привычными организационными мерами, т.е. практически «бесплатно». А, например, на сетевом уровне для защиты сложных систем необходимо применение уже достаточно дорогостоящих технологий, таких как межсетевое экранирование, VPN, средства обнаружения вторжений и т.д.

Одним из главных преимуществ представления СЗИ в виде иерархии функционально-независимых уровней является существенное упрощение процесса проектирования системы, поскольку теперь проектирование одной многофункциональной и сложной системы можно разложить на несколько законченных этапов проектирования гораздо менее сложных систем для каждого уровня в отдельности и завершающего этапа контроля целостности системы защиты при переходе от уровня к уровню. В том случае, когда целостность системы защиты сохраняется, СЗИ в целом может считаться комплексной.

Следует отметить, что предлагаемый пятиуровневый «стековый» подход помимо упрощения самого процесса проектирования, позволяет четко формализовать три достаточно сложные задачи, которые неизбежно возникают при создании систем защиты ИС:

- обеспечение целостности (комплексности) системы защиты;
- разграничение требований и функций СЗИ при защите информации, обладающей различной степенью конфиденциальности;
- обеспечение целостности СЗИ при защите территориально-распределенных ИС.

При этом при решении указанных задач в абсолютном большинстве случаев удается обеспечить оптимальное соотношение функциональность/стоимость СЗИ для владельца ИС и должным образом это обосновать.

Проблема обеспечения целостности системы защиты в рамках предложенной модели СЗИ принимает достаточно понятную и наглядную форму – это, как уже было сказано, обеспечение полноты реализации функций защиты на каждом уровне модели СЗИ и обеспечение целостности функций защиты при переходе от уровня к уровню. Очевидно, что максимальная степень комплексности СЗИ достигается в том случае, когда применяемые технические средства, решения и методы обеспечивают защиту каждого уровня в соответствии с самыми жесткими требованиями и при этом все используемые с СЗИ технические средства проявляют свою функциональность на каждом уровне модели. Очевидно, что построить настолько «комплексную» СЗИ в принципе возможно только

при неограниченных ресурсах проекта. Поэтому на практике необходимо найти разумный и, главное, обоснованный компромисс между «комплексностью» системы, т.е. ее функциональной наполненностью, и совокупной стоимостью ее построения и эксплуатации. Под стоимостью эксплуатации подразумевается уровень адаптируемости СЗИ (т.е. сохранение необходимого уровня защиты) к неизбежным изменениям состава и конфигурации ИС.

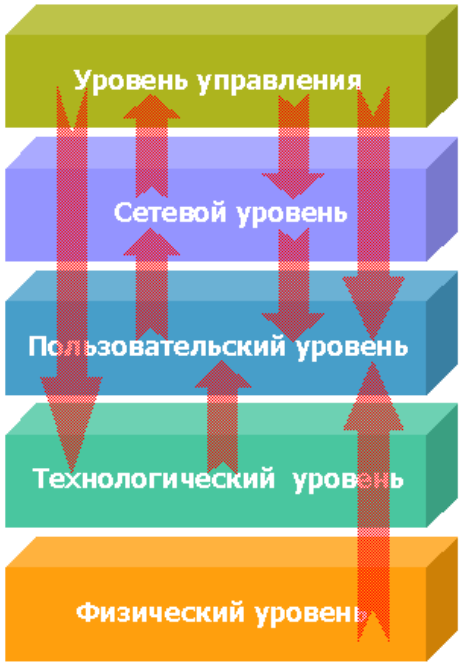

Рис.1. Пример реализации функциональных связей между уровнями СЗИ.

Практика работы компании ЭЛВИС+ показывает, что в настоящее время оптимальным подходом для обеспечения необходимой комплексности СЗИ является построение системы на базе таких продуктов, которые проявляют свои защитные функции на двух-трех, при этом не обязательно соседних, уровнях СЗИ (Рис.1). И, очевидно, «проявляемые» на каждом уровне защитные функции должны полностью перекрывать налагаемые на защиту данного уровня требования. Сделать это возможно уже сегодня на основе имеющихся на российском рынке продуктов по защите информации. Так, например, существующие сегодня развитые продукты по реализации функций межсетевого экранирования (например CheckPoint FW-1) позволяют решать не только традиционные для межсетевых экранов задачи по фильтрации трафика на сетевом уровне, но и часть задач пользовательского уровня (аутентификация удаленных пользователей и задание политик безопасности для каждого пользователя при работе в открытой сети), технологического уровня (контроль входящего трафика на предмет наличия разрушающих и вредоносных программ) и уровня управления (целостное управление всем комплексом с единой консоли). Очевидно, что чем больше таких «многоуровневых» средств защиты применяется в СЗИ, тем легче ее проектирование и полнее и надежнее она выполняет свои функции.

Проблема разграничение системы защиты информации различной степени конфиденциальности заключается в том, что часто на практике в рамках одной ИС приходится «работать» с информацией, требования по защите которой существенно отличаются друг от друга. Так обрабатываемые и хранимые в рамках типовой ИС информационные ресурсы, как правило, разделяются на три группы:

- **открытые информационные ресурсы,** которые хотя и не содержат конфиденциальной информации в явном виде, но, тем не менее, должны быть в минимально-необходимой мере защищены от внешнего НСД;
- **конфиденциальные информационные ресурсы**, содержащие экономическую, финансовую, коммерческую, производственную и другую действительно конфиденциальную информацию, раскрытие или уничтожение которой может нанести реальный ущерб компании. Как известно, требования по защите этих ресурсов определяются владельцем информации и они, очевидно, должны быть существенно жестче требований к защите информации первой группы;
- **информационные ресурсы ограниченного доступа,** требования по защите которых регламентируется законодательством РФ (персональные данные, сведения, содержащие государственную тайну и др.)

Очевидно, что защита всех трех разновидностей информационных ресурсов в рамках одной и той же СЗИ подразумевает, что даже открытые ресурсы будут защищаться по требованиям, предъявляемым к защите секретной информации. Очевидно, это приведет к необоснованно высокой стоимости СЗИ и большим неудобствам работы для персонала компании. Так же неэффективно будет построение трех различных СЗИ для каждого из ресурсов, поскольку, во-первых, четко разделить эти ресурсы в рамках одной КИС практически никогда не удается, а во-вторых, это опять приведет к повышению стоимости самой системы.

В рамках предложенной модели указанная проблема может быть решена путем разграничения требований и, соответственно, функциональности для каждого из уровней защиты СЗИ применительно к каждой группе информационных ресурсов. Сделать это тем более возможно, поскольку в пределах одного уровня требования к защите информации находятся, можно сказать, «в одной системе координат». Например, применительно к защите информации на пользовательском уровне требования по контролю доступа к открытой информации могут вообще не выдвигаться; для доступа к конфиденциальной информации может выдвигаться уже определенная внутрикорпоративная система требований (разграничение доступа средствами ОС и СУБД на основе паролей, создание контрольных групп пользователей и т.д.); для защиты информации третьей группы – строгая система требований в полном соответствии с требованиями законодательства. При этом, если информационные ресурсы в каком либо элементе ИС (помещение, сервер БД, канал связи, сегмент ЛВС и т.д.) четко физически не разделены, в рамках СЗИ необходимо оценить возможность разделения указанных ресурсов на каждом из уровней системы. Если в пределах одного уровня сегментировать информацию не удается, система требований для данного уровня, очевидно, должна строиться исходя из требований по защите информации максимальной степени конфиденциальности. Если сегментация информации возможна, к уровню может предъявляться двойная (тройная и т.д.) система требований.

Применительно к серверу БД это означает, что если на данном сервере одновременно хранится, например, открытая и конфиденциальная информация, то вероятнее всего все требования физического, технологического и сетевого уровней должны исходить из того, что уровень защищаемой на сервере информации – конфиденциальный. На пользовательском уровне информационные ресурсы, скорей всего, удастся разделить по правам доступа для различных групп пользователей, поэтому для этого уровня может предъявляться двойная система требований. В тех случаях, когда объем открытой информации на сервере существенно превышает объем конфиденциальной информации, а следовательно, уровень защиты для нее избыточен,

может иметь смысл перенести конфиденциальную информацию на другой сервер. В подобных случаях необходимо применение несложных экономических расчетов по оценке эффективности того или другого решения.

Проблема обеспечения целостности защиты территориально-распределенных КИС заключается в том, что, как правило, даже большая корпорация не в состоянии обеспечить одинаковый уровень защиты для ИС Центрального офиса (ЦО) компании и всех ее филиалов (представительств, дочерних компаний и т.д.). На практике чаще всего ЦО защищается в соответствии с самыми жесткими требованиями по ИБ, а для системы защиты филиалов регламентируются только технические параметры взаимодействия с СЗИ ЦО. В большинстве случаев такой подход является вполне обоснованным, поскольку именно в ИС ЦО сосредоточены основные информационные ресурсы компании. Поэтому проблема, собственно, заключается в том, чтобы обеспечить целостность защиты СЗИ ЦО при ее информационном взаимодействии с СЗИ «менее защищенных» филиалов.

В рамках предложенного подхода сохранение целостности защиты корпоративной СЗИ обеспечивается в том случае, когда при взаимодействии двух систем СЗИ ЦО дополнительно контролирует те параметры защиты, которые не контролируются в СЗИ филиала. В случае же «прозрачного» взаимодействия двух систем на одном из уровней СЗИ (чаще всего пользовательском и сетевом) требования к данному уровню СЗИ филиала должны соответствовать аналогичным требованиям СЗИ ЦО.

Например, если в рамках корпоративной ИС реализовано «прозрачное» взаимодействие ИС ЦО и филиалов посредством, например, VPN технологии, и при этом СЗИ филиала не обеспечивает гарантированную целостность своих информационных ресурсов, то технические средства сетевого уровня СЗИ ЦО должны в обязательном порядке контролировать «качество» приходящей из филиала информации и аутентичность запросов на доступ к корпоративным информационным ресурсам.

В заключение еще раз подчеркнем, что предлагаемый подход к проектированию СЗИ на базе иерархической пятиуровневой модели носит достаточно общий (методический) характер и оставляет большое поле для творчества компаниям-проектировщикам. Тем не менее, как показывает опыт компании ЭЛВИС+, такой системный подход позволяет существенно сократить сроки разработки СЗИ и при этом предложить заказчику действительно оптимальное и обоснованное решение.