ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НАЧИНАЕТСЯ НА УРОВНЕ БИЗНЕС-ПРОЦЕССОВ.

Интервью менеджера по работе с партнерами ОАО «ЭЛВИС+» Березина А.С. корреспонденту журнала «Connect. Мир связи»

Проблема обеспечения безопасного ведения бизнеса с использованием новых информационных технологий и глобальных информационных сетей – одна из самых острых сегодня не только в России, но и в во всех развитых странах мира. Потери от различного рода правонарушений в сетях оцениваются уже в сотни миллионов долларов. В каком состоянии находится российский рынок систем защиты информации (СЗИ), отличается ли он от мирового рынка – об этом корреспондент журнала попросил рассказать *Андрея Березина, руководителя направления по работе с партнерами компании «ЭЛВИС+»*

Корр.: Прежде чем начать разговор о рынке СЗИ, предлагаю определиться с кругом понятий. Информационная безопасность и защита информации – это одно и то же?

Нет, это разные понятия. Сегодня под защитой информации понимается, в общем случае, некий законченный набор организационных и технических мер по обеспечению доступности, целостности и конфиденциальности информации, циркулирующей в рамках корпоративной информационной системы (ИС).
Информационная безопасность представляет собой более широкий комплекс мер, включающий в том числе и защиту информации. Она преследует более глобальную цель: обеспечить в рамках компании некую доверенную информационную среду или, как сейчас стало модно говорить, единое информационное пространство, которая позволит компании успешно работать в сложившихся условиях ее окружения. Под последними могут пониматься как банальные перебои с электропитанием, так и активное информационное противодействия со стороны конкурентов.
Таким образом можно сказать, что защита информации - это обеспечение информационной безопасности компании на уровне ИС.

Корр.: Можно ли каким-то образом квалифицировать системы защиты информации?

Недавно я слышал попытку квалифицировать ИС как защищенные, надежно защищенные и гарантированно защищенные. Считаю, что подобно булгаковской "осетрине второй свежести" ИС предприятия является либо защищенной, либо нет. Может быть имеет смысл проводить квалификацию СЗИ с технологической или организационной точек зрения. В таком случае, на мой взгляд, можно выделить четыре основных типа или, точнее, этапа развития таких систем:

- Однокомпонентные системы, которые строятся на базе одного, как правило, узкоспециализированного продукта по защите информации.
- Многокомпонентные системы, строящиеся 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 связаны между собой (ни технологически, ни организационно).
- Комплексные системы защиты, представляющие собой дальнейшее развитие многокомпонентных СЗИ, где используемые продукты, технологии и решения объединяются на организационном уровне, с тем чтобы обеспечить максимальную степень защищенности всей корпоративной ИС в целом. Очевидно, что при этом надежность всего комплекса эквивалентна стойкости самого слабого его звена.
- Интегрированные СЗИ, в которых все элементы защиты объединяются (интегрируются) не только на организационном, но и на техническом и даже технологическом уровнях. В таком случае компрометация одного из элементов защиты должна надежно компенсироваться противодействием других ее элементов.

На мой взгляд, построение по-настоящему интегрированных СЗИ сегодня пока еще невозможно по техническим причинам. Стало быть, оптимальным решением можно считать построение комплексных СЗИ.

Корр.: Чем определяется надежность (эффективность) СЗИ? Существует ли методика оценки эффективности СЗИ?

Конечно же, существуют достаточно строгие и сложные методики оценки эффективности СЗИ, основанные на анализе архитектуры системы, прогнозе финансовых рисков и т.п. Но это отдельная тема. В двух словах я бы ответил на Ваш вопрос таким образом: эффективность корпоративной СЗИ заключается в том, чтобы …… компания не замечала ее эффективности. СЗИ должна работать максимально «прозрачно» для компании и при этом обеспечивать максимальный уровень защиты информации. Другими словами эффективная СЗИ не должна «напоминать» о своем существовании: пользователям - какими-то неудобствами в работе; руководству - фактами утечки конфиденциальной информации. На мой взгляд этого можно добиться только в том случае, если СЗИ достаточно тесно технологически интегрирована в корпоративную ИС, а организационно – в структуру рабочих процессов компании.

Корр.: Получается, что решение по обеспечению информационной безопасности предприятия неразрывно связано с процессами автоматизации?

Совершенно верно. Невозможно отдельно заниматься организацией или оптимизацией бизнес-процессов, затем отдельно их автоматизировать, а затем еще и отдельно их защищать. Вернее поступить таким образом, конечно, можно (и так, к сожалению, в большинстве случаев и делается), но положительного результата при этом, как правило, не получается – система «расходится». На практике это означает, что сначала ИС не «уживается» с рабочими процессами, а затем еще и СЗИ постоянно «вмешивается» в работу. Это, оказывается, можно; а это, оказывается, нельзя; а это теперь нельзя в принципе…. В итоге компания теряет эффективность, несмотря на полную автоматизацию и защиту.

Приведу простой пример. Одной из первых задач, решаемых при создании СЗИ, является категорирование корпоративной информации и разграничение прав доступа к ней различных сотрудников компании. Очевидно, что ИС должна изначально строится исходя из последующих требований по проведению такого категорирования и разграничения. Но такая информация сама по себе не появится – она следует из анализа и «настройки» рабочих процессов.

К сожалению очень часто бывает, что бизнес-процессы в компании организованы не самым оптимальным образом, вследствие чего через какую-то точку в структуре компании проходит информация, которая в данной точке для работы совершенно не нужна. Или, того хуже, в данной точке смешиваются потоки разных уровней конфиденциальности. ИС четко повторяет эту ошибку, в результате чего создается уязвимость, справится с которой возможно только уменьшением эффективности СЗИ или чрезмерным увеличением ее стоимости. С уверенностью можно сказать, что информационная безопасность начинается на уровне бизнес-процессов.

Корр.: Есть ли различия между российским подходом к проблеме защиты информации и методами, используемыми в США и Европе?

Вопрос сложный. Я бы сказал, что основное различие заключается в некоторой «самостийности» российского рынка защиты информации. Проявлений этой самой «самостийности» можно отметить довольно много.

Первое проявление, например, касается подхода к разработке средств защиты информации. Запад уже давно понял, что всеобщая (и добровольная!) стандартизация в области информационных технологий обеспечивает более высокую надежность ИС, преемственность платформ, совместимость и комплексность решений, колоссальную свободу выбора и, самое главное, способствует сохранению инвестиций. Открытый стандарт, в т.ч. и в области защиты информации, для западного менталитета означает, что над ним потрудились умы лучших специалистов, он всесторонне протестирован, своевременно дополняется и совершенствуется. То есть на сегодняшний день он идеально соответствует потребностям рынка. В России такого доверия открытым стандартам и продуктам на их базе пока нет, хотя опыт последних двадцати лет вроде бы как и не оставил альтернатив открытым стандартам.

Второе проявление более серьезно и заключается, на мой взгляд, в излишней законодательной «зарегулированности» российского рынка защиты информации, которая тем не менее не дает

четкую и целостную правовую картину того, что «можно», а что «нельзя». Вернее сказать, что именно «нельзя» – известно, но что за это будет – большой вопрос. В результате получается парадокс: защищать свою конфиденциальную информацию все обязаны, но построить нормально работающую СЗИ в рамках правового поля практически невозможно. Одним из ключевых вопросов по-прежнему остается криптография. Ведь сегодня фактически каждый IT-продукт в той или иной форме содержит криптографию; в большинстве случаев она жестко встроена в продукт. Поэтому пользователь по существу стоит перед альтернативой: либо работать на уровне DOS, либо нарушать закон.