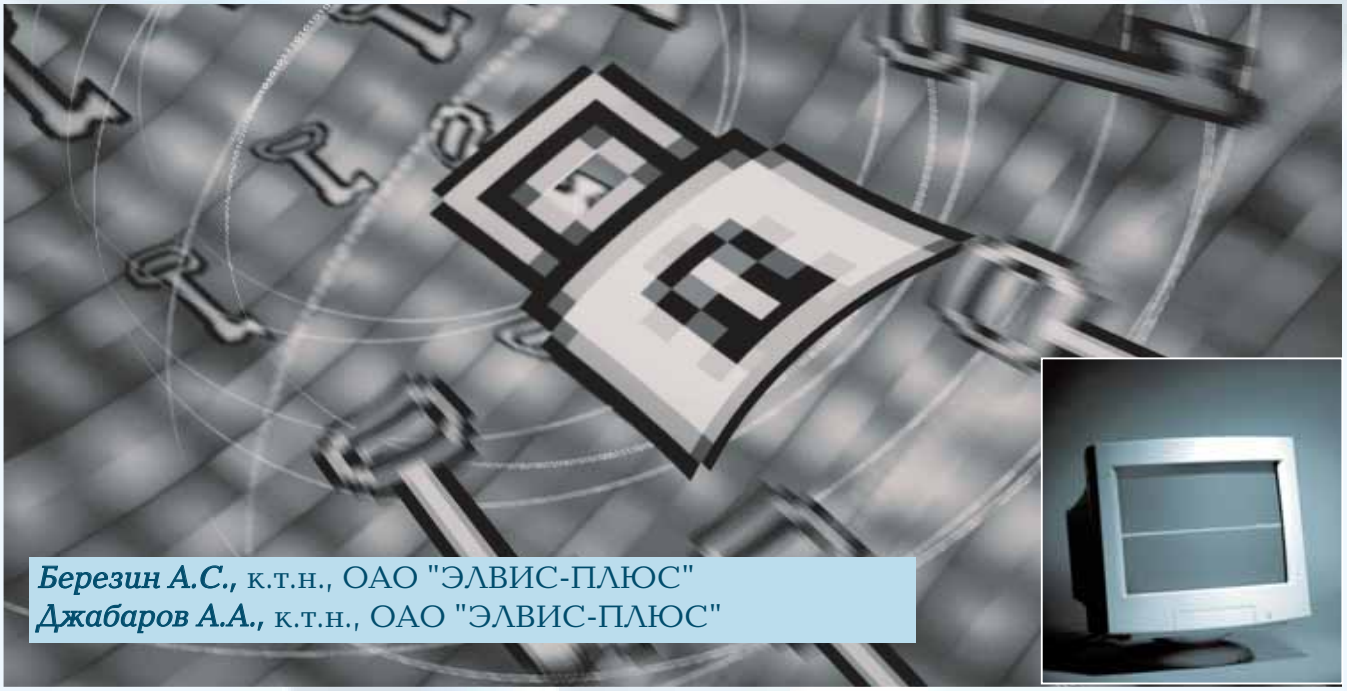
К вопросу создания подсистемы информационной безопасности при модернизации корпоративной сети



Березин А.С., к.т.н., ОАО "ЭЛВИС-ПЛЮС"
Джабаров А.А., к.т.н., ОАО "ЭЛВИС-ПЛЮС"

Зачем это нужно?

Продумывая программу модернизации корпоративной сети (КС), сегодня любой грамотный IT-менеджер обязан задуматься о модернизации (а, может быть, и о создании) подсистемы информационной безопасности (ПИБ) своей КС. При этом под ПИБ не следует понимать сверхсложную систему защиты от атак какого-то злонамеренного и суперпрофессионального хакера. Не меньшей, а часто гораздо большей вред информационным ресурсам (ИР) КС могут нанести неосторожные действия абсолютно лояльных сотрудников, непреднамеренно получивших доступ к критичной для отрасли информации.

Можно выделить целый ряд причин, по которым стоит задуматься о информационной безопасности (ИБ) КС. Во-первых, разнообразные функции обеспечения ИБ сегодня достаточно сильно интегрированы в существующие продукты и технологии построения корпоративных информационных и телекоммуникационных систем, поэтому не использовать эти возможности просто неразумно. Во-вторых, современный бизнес невозможен без активного использования публичных сервисов, предоставляемых открытыми сетями связи и, прежде всего, Интернет. По этой причине КС тем или иным способом необходимо подключать к открытым сетям, что опять же неразумно делать без обеспечения безопасности этого соединения. В-третьих, грамотно спроектированная и аккуратно реализованная ПИБ сможет существенным образом расширить функциональные возможности самой КС: построение системы удаленного защищенного доступа мобильных сотрудников к информационным ресурсам КС; использование дешевых Интернет-коммуникаций для передачи информации между различными подразделениями компании; построение системы компьютерной телефонии и т.д. И, наконец, чаще всего стоит просто задуматься о стоимости накопленных за многие годы ИР, хранимых и обрабатываемых в рамках КС, или о степени влияния оперативности и достоверности получаемой информации на качество принимаемых решений. Другими словами, требование обеспечения ИБ КС сегодня можно смело считать обусловленным простым здравым смыслом!

Что такое ПИБ?

Для успешного выполнения поставленной задачи проектировщик ПИБ прежде всего должен четко представлять себе эту систему на самом общем, концептуальном уровне с тем, чтобы правильно определить основные приоритеты ее построения и взаимосвязь между ее отдель-

ными компонентами. Для этого попробуем построить упрощенную модель ПИБ КС на базе "исторического подхода", т.е. типовых этапов ее построения. Такой подход интересен тем, что, во-первых, именно так стоятся большинство ПИБ на практике, во-вторых, это даст нам возможность экстраполировать результаты моделирования на ближайшее будущее.

Итак, построение любой КС начинается с установки рабочих станций, следовательно, ПИБ КС начинается с защиты именно этих объектов. Для этого можно (и нужно!) использовать всем давно и хороши известные штатные средства защиты операционных систем (ОС); антивирусные пакеты; дополнительные устройства аутентификации пользователя и средства защиты рабочих станций от НСД; средства шифрации прикладного уровня т.д. На базе перечисленных средств защиты информации (СЗИ) стоится первый уровень ПИБ КС - уровень защиты рабочих станций сети (см. рис.1).

На втором этапе развития КС (который на практике часто происходит одновременно с первым) отдельные рабочие станции объединяются в локальные сети, устанавливаются выделенные сервера и (это случается сегодня все чаще и чаще) организуется выход из локальной сети в Интернет. На данном этапе "в бой" вступают СЗИ второго уровня - уровня защиты локальной сети: средства безопасности сетевых ОС; средства разграничения доступа к разделяемым ИР; средства защиты домена локальной сети; сервера аутентификации пользователей; межсетевые экраны (МЭ) и proxy-серверы; средства организации VLAN; средства обнаружения атак и уязвимостей защиты локальной сети и т.д. Очевидно, СЗИ второго уровня гораздо более сложны технологически, нежели СЗИ первого уровня, что, естественно, отражается на их стоимости и трудоемкости установки и сопровождения.

Третий этап развития КС, который активно развивается в настоящее время, состоит в объединении локальных сетей нескольких филиалов компании в общую корпоративную intranet-сеть на базе современных IT-технологий поддержки QoS (ATM, FR, DiffServ, MPLS и др), используя в качестве коммуникационной среды публичные сети, включая, конечно, и Интернет. При этом безопасность обмена информацией через открытые сети обеспечивается применением технологий Virtual Private Network (VPN), которые и составляют основу третьего уровня ПИБ КС. VPN технологии, как правило, достаточно глубоко интегрированы со СЗИ первого (средства аутентификации пользователя и защиты от НСД) и второго (МЭ и сетевые ОС) уровней и защищенный VPN-канал может "доходить" не только до маршрутизаторов доступа и пограничных МЭ, но и до конкретных серверов и рабочих станций локальной сети, составляя, таким образом, своего рода "скелет" ПИБ КС.

Что же ожидает КС в ближайшие 5-10 лет? Четвертым этапом развития КС будет, видимо, организация защищенного ***межкорпоративного*** обмена информацией (externet-сети), который потребует качественно новых технологий обеспечения ИБ для работы "всех со всеми", т.е., другими словами, для формирования системы электронного бизнеса. В качестве технологической и методологической основы для создания инфраструктуры е-бизнеса наиболее вероятным кандидатом является группа технологий и методов, позволяющих строить системы управления публичными ключами и сертификатами - Public Key Infrastructure (PKI). Соответственно, PKI, скорей всего, является последним ***количественным*** уровнем уровнем ПИБ КС.

Здесь следует особо подчеркнуть следующее. Как известно, PKI - это по сути лишь группа IT-технологий поддержки работоспособности довольно сложной административной системы, которая призвана выполнять всего две функции (но в рамках всей страны и даже, в перспективе, планеты!): 1) генерация и корректное (протоколированное) распространение ключей и сертификатов; 2) отслеживание "жизненного цикла" выданных ключей и сертификатов в режиме реального времени. Очевидно, что после получения от PKI необходимых параметров, построение защищенного информационного обмена между отдельными компаниями (вернее - их КС) будет строиться на базе совсем других технологий, и прежде всего технологий поддержки электронно-цифровой подписи (ЭЦП) и VPN. Таким образом, с технической точки зрения е-бизнес станет возможен только в том случае, если используемые "внешние" СЗИ (т.е. СЗИ 2 и 3 уровней) различных компаний будут "понимать" не только друг друга, но и соответствующие приложения PKI некоторой заранее неизвестной (по крайней мере для одной из компаний) третьей стороны. Очевидно, что такое возможно только в том

Рис. 1. Четырехуровневая модель подсистемы информационной безопасности корпоративной сети

случае, когда все упомянутые средства являются ***совместимыми***, что в условиях глобальной природы е-бизнеса может означать только одно - все они построены на базе открытых мировых стандартов. Применительно к нашей конкретной задаче это означает, что если ваша компания планирует свое участие в е-бизнесе, необходимо изначально строить ПИБ на базе открытых стандартов (благо сегодня это сделать совсем несложно, т.к. абсолютное большинство производителей СЗИ сегодня ориентируются именно на открытые стандарты).

Следует заменить, что применительно к ИБ КС проблема совместимости различных СЗИ актуальна не только по причине "заманчивости" перспектив е-бизнеса. Хорошо известно, что ПИБ - это "по определению" комплексная система, состоящая из большого числа отдельных элементов, выполняющих свои определенные функции. Такая система может быть надежной (а именно это является основным качеством и главной целью создания ПИБ) только в случае ее глубокой ***интегрированности.*** Другими словами, стойкость ПИБ не должна зависеть от стойкости самого "слабого" СЗИ (хотя именно такой принцип главенствует в настоящее время); в интегрированной ПИБ компрометация одного из элементов защиты должна надежно компенсироваться противодействием других ее элементов, что может быть обеспечено только их слаженной работой в рамках ***единой*** системы. К сожалению, на современном этапе развития технологий ИБ использование явления синергизма в масштабах всей корпоративной ПИБ пока еще невозможно в силу незрелости открытых стандартов и отсутствия четко выраженного требования рынка. Однако, тенденция развития СЗИ в этом направлении уже прослеживается достаточно явно: объединение средств защиты от НСД со средствами шифрации прикладного уровня; интеграция МЭ с антивирусными пакетами и VPN; средств аутентификации с технологиями PKI и т.д.

Возвращаясь к построенной нами модели ПИБ КС хочется сделать еще одно важное наблюдение. Первые три уровня "пирамиды" можно отнести к СЗИ в традиционном их понимании, поскольку эти средства призваны обеспечить собственную ИБ КС. Верхние два уровня явно относятся уже к уровню обеспечения е-бизнеса, поскольку VPN служат для построения защищенного обмена информацией между компаниями, а PKI обеспечивает VPN устройства необходимыми для формирования защищенных каналов параметрами (ключами и сертификатами). Таким образом, как мы видим, VPN технологии ***исторически*** позиционированы в качестве "связующего" элемента между чисто внутрикорпоративной задачей - обеспечение ИБ распределенной КС, и глобальной бизнес-задачей компании - обеспечение интеграции в систему мирового электронного бизнеса 21 века!

Строим ПИБ

Как показывает опыт, построение ПИБ КС далеко не всегда является сугубо технической задачей. Гораздо чаще она представляет собой задачу организационно-техническую, в которой от решения организационной составляющей во многом зависит состав и сложность реализации составляющей технической. В общем случае, построение ПИБ КС целесообразно разделить на несколько этапов.

На первом этапе рекомендуется провести четкую классификацию существующих ИР компании по степени их конфиденциальности. Мы намеренно не рассматриваем случай, когда среди корпоративных ИР существует информация, составляющая государственную тайну или коммерческую тайну другой компании (материнской компании, компании-партнера, заказчика и т.д.). Это особый (и достаточно сложный!) случай, который необходимо рассматривать отдельно. Но, в рамках любой компании вполне обоснованным является требование о придании информации, например, финансового отдела или отдела разработки статуса конфиденциальной информации, доступ к которой необходимо ограничить прежде всего для сотрудников самой компании[1]. Эту задачу, как правило, можно решить как организационными методами, так и техническими средствами, однако наиболее эффективным способом является применение некого комбинированного решения. В последних двух случаях, скорей всего, потребуется пересмотр (или переконфигурирование) топологии существующих локальных сетей или up-grate сетевого оборудования с тем, чтобы иметь возможность четко выделить те сегменты КС, в которых обрабатывается конфиденциальная информация, а также ограничить число (контролируемых!) точек взаимодействия этих сегментов с остальными сегментами КС. Взаимодействие с открытыми сетями рабочих станций и серверов этих сегментов, если это необходимо, лучше всего организовать не напрямую, а через доверительную среду КС.

[1]Данное требование актуально по той причине, что согласно мировой статистике абсолютное большинство (до 90%) случаев НСД к ИР КС происходит именно из внутренних сетей.

На втором этапе необходимо сформировать собственную политику безопасности КС в виде, например, некой системы требований к ПИБ применительно именно к данной компании. Скорей всего, без надлежащего опыта это удастся сделать лишь на самом общем уровне - часто недостаточном для решения данной задачи. На самом деле, делать этого и не нужно, поскольку как отечественными, так и западными специалистами по ИБ уже составлены необходимые документы, в которые четко классифицируются разные уровни обеспечения ИБ КС и необходимые для этого технические средства, а также организационные мероприятия. Можно, например, рекомендовать комплект "Руководящих документов" Гостехкомиссии при Президенте РФ http://www.infotecs.ru/gtc/default.htm или более "развернутый" документ "Evaluation criteria to IT Security" http://csrc.nist.gov/cc/ccv20/ccv2list.htm Взяв за основу перечисленные там требования, можно в большой степени быть уверенным в том, что необходимая комплексность ПИБ КС будет обеспечена. На данном этапе нелишним будет снова задуматься о перспективах развития КС, например, с какими из партнеров или заказчиков планируется строить защищенные взаимодействия в ближайшие пять лет? Очевидно, что со-

Таблица 1

№	Наименование функции ПИБ КС	Штатные средства ОС	Антивирусные средства	Средства защиты от НСД	Средства сетевого экранирования прикладного уровня	Сервер аутентификации пользователей	VLAN	Межсетевые экраны	Средства обнаружения уязвимостей	VPN
1.	Защита АРМ пользователя рабочей станции от НСД									
1.1.	Аутентификация пользователя	X		X		X				
1.2.	Разграничение доступа к АРМ рабочей станции	X		X		X	X			
1.3.	Защита АРМ рабочей станции		X		X				X	
2.	Защита локальной сети									
2.1.	Разграничение доступа к защите защищаемым АРМ	X		X	X	X	X		X	X
2.2.	Защита внутренних каналов связи				X		X			X
2.3.	Сегментирование локальной сети						X	X		X
3.	Защита межсетевого взаимодействия									
3.1.	Защита от удаленных атак		X		X			X	X	X
3.2.	Защита внешних каналов связи				X					X

став и "жесткость" требований к вашей ПИБ должен быть как минимум не ниже соответствующих параметров ПИБ вашего партнера или заказчика.

На третьем этапе можно приступить непосредственно к выбору технических средств, которые в совокупности с организационными мерами позволили бы успешно решать поставленные перед ПИБ задачи. Некоторым ориентиром для выполнения этого этапа работ может служить таблица №1, в которой рассмотрено (в первом приближении) соответствие наиболее популярных СЗИ общим требованиям по защите корпоративных информационных систем (или функциональности ПИБ КС).

Следует заметить, что наличие "крестиков" в одной строке таблицы для различных СЗИ отнюдь не означает, что эти СЗИ являются полностью взаимозаменяемыми. Например, задачу защиты локальной сети от атак извне (см. п.3.1. таблицы №1) обозначенные пять СЗИ решают абсолютно по-разному, закрывая, таким образом, свою часть "дыр" в защите локальной сети. Очевидно, что максимальную надежность ПИБ можно обеспечить лишь путем применения максимально комплексного решения, что на практике, к сожалению, не всегда возможно. Поэтому искусство проектировщика ПИБ на данном этапе заключается в том, как "меньшими средствами решить большую задачу".

При окончательном выборе уже конкретного СЗИ конкретного производителя, на наш взгляд, помимо базовых требований к продукту (набор функциональности; относительная стоимость необходимых функций; совместимость с другими СЗИ; условия технической поддержки продукта производителем или дистрибьютором и т.д.) необходимо уделить внимание следующим двум критериям:

1) Быстродействие данного СЗИ;

2) Наличие сертификата соответствия.

Требование по быстродействию СЗИ относится, главным образом к средствам защиты межсетевого взаимодействия (МЭ, proxy-сервера, VPN устройства), поскольку именно здесь, как правило, возникает жесткое требование к скорости обработки информации. Прежде всего это относиться к СЗИ, применяющим методы криптографического преобразования (кодирования) информации (средства шифрации прикладного уровня, VPN-устройства и др.), поскольку подобная обработка трафика в реальном масштабе времени требует очень серьезных вычислительных ресурсов, которые необходимо предварительно оценить.

Наличие сертификата соответствия на выбранное СЗИ является строго обязательным, вообще говоря, только для государственных учреждений, а также для тех негосударственных учреждений, которые используют информацию, отнесенную государством (в рамках существующего законодательства) к конфиденциальной (секретной) информации. Например для учреждений, работающих по государственному заказу, или имеющих доступ к персональной информации граждан, или сведениям о добыче и обработке стратегических полезных ископаемых и т.д. Прочие организации при построении ПИБ своих КС могут использовать как сертифицированные, так и несертифицированные СЗИ. Многие компании (и не без оснований) считают, что "настоящий брэнд" лучше всякого сертификата, и потому об этом просто не задумываются.

На самом деле, процедуру сертификации СЗИ государственными органами необходимо воспринимать не более чем элемент государственного механизма, призванного осуществлять защиту прав потребителя, который должен, в принципе, одинаково эффективно защищать право потребителя есть качественную колбасу и использовать качественные СЗИ. Применительно к практике построения ПИБ это означает, что если вы применили несертифицированные СЗИ и вашу систему "взломали", то ответственность за это несете только вы. В этом случае привлечь производителя СЗИ к ответственности, тем более материальной, удается крайне редко. Если же вашу ПИБ взломали "по вине" сертифицированных СЗИ, то бремя ответственности перекладывается "на плечи" сертифицирующего государственного органа, т.е., читай, на государство, и уже государство обязано задействовать всю мощь гражданского, арбитражного и уголовного права для защиты интересов собственника информации, наказания виновных и возмещения понесен-

ных убытков. К сожалению, эта сама по себе прекрасная идея в России еще не доведена до работающего механизма, хотя определенные и заметные усилия в этом направлении уже явно прослеживаются.

Пока же сертификат соответствия на СЗИ, или хотя бы возможность его получения для "любимого брэнда" в принципе, можно считать необходимым в случаях, если 1) вам хочется убедиться (или убедить своего начальника!) в том, что данное СЗИ является тем, что о нем говорит производитель; 2) СЗИ соответствует тому классу защищенности, который требуется для защиты информации вашего уровня конфиденциальности; 3) в ходе выполнения работ необходимо документирование возможностей вашей ПИБ для представления, например, партнеру, органу по аттестации, или (почему бы и нет!?) страховой компании.

Для тех компаний, которые (по разным причинам) изначально ориентируются только на сертифицированные СЗИ, необходимо также иметь в виду, что СЗИ, использующие методы криптографического преобразования информации (СКЗИ), в общем случае должны иметь два сертификата:

- сертификат соответствия, выдаваемый Гостехкомиссией при Президенте РФ, который подтверждает соответствие технической реализации СЗИ нормативным требованиям "Руководящих документов" самой Гостехкомиссии, степень соответствия ТУ на данный продукт, отсутствие в продукте недекларированных возможностей, "тайных ходов" и т.д.
- сертификат соответствия, выдаваемый ФАПСИ, который подтверждают корректность реализации того модуля продукта, который реализует функции криптографического преобразования информации, или всего продукта, если эти функции "жестко" встроены в продукт.

Кроме того, сертификат Гостехкомиссии может быть одного из трех видов:

- сертификат на конкретный образец изделия;
- сертификат на партию изделий;
- сертификат на производство изделий.

Преимущества последнего сертификата очевидны, поскольку компания может закупать любое количество продуктов и все они будут автоматически иметь сертификат. Первые два типа сертификата означают, что за сертификацию необходимого комплекта продуктов необходимо платить дополнительно (стоимость сертификата либо включена в стоимость продукта, либо, чаще всего, оплачивается отдельно как дополнительная опция).

Сертификат на производство до сих пор имеют только отечественные СЗИ, и видимо, это правило сохраниться до тех пор, пока западные производители не перенесут свое производство на территорию РФ. Кроме того необходимо иметь в виду, что сертификаты западных продуктов при одинаковой или даже большей функциональности, как правило, гораздо "слабее" сертификатов отечественных СЗИ, поскольку западные производители, например, не "горят желанием" предоставлять исходные коды своих программ на сертификацию в Россию. По этой же причине, а также по причине отсутствия реализации отечественного криптоалгоритма ГОСТ 28147-89, западным СКЗИ крайне затруднительно получить сертификат ФАПСИ.

Однако, вернемся к построению ПИБ. После того, как на основе выбранных организационных и технических требований удалось определить круг необходимых СЗИ (СКЗИ), наконец-то настало время этапа технического проектирования ПИБ и всех хорошо известных последующих этапов, ведущих к вводу готовой системы в эксплуатацию. Заметим только, что для некоторых типов компаний (обозначенных ранее) этапу ввода ПИБ в эксплуатацию должен предшествовать этап проведение аттестации ПИБ на соответствие требованиям, налагаемым российским законодательством к системам защиты отдельных категорий информации. И только после подтверждения корректности реализации ПИБ внешним государственным органом, систему можно вводить в эксплуатацию.

Итого

Спроектировать и построить бронированный автомобиль гораздо сложнее, чем автомобиль обычный. Поэтому ни у кого не возникает вопросов, почему первый стоит в несколько раз дороже второго. Аналогично, защищенная КС должна стоить дороже незащищенной КС, при этом "количество раз" зависит как от требований внутрикорпоративной политики безопасности, так и от спектра применяемых СЗИ. Однако на практике следует стремиться к тому, чтобы стоимость ПИБ не превышала 10-20% от стоимости самой КС.

Житейская мудрость говорит о том, что сделать "с нуля" всегда легче и дешевле, чем переделывать готовую систему заново. Поэтому вопрос о построении ПИБ КС целесообразно поднимать именно на этапе модернизации КС, когда еще возможно учесть требования политики безопасности на уровне топологии КС и тем самым, сэкономить довольно значительную часть материальных средств. Дополнительным источником экономии может служить вариант построения ПИБ силами компании - системного интегратора, которая проводит основной объем работ по модернизации КС. Проблема с выбором такого системного интегратора сейчас практически не стоит, поскольку большинство таких компаний в настоящее время активно расширяют свой традиционный бизнес в строну построения ПИБ КС. Очевидно, что привлечение сторонней компании к построению ПИБ не должно снижать стойкость самой системы, в т.ч. и за счет возможной утечки информации. Для этого, как правило, достаточно "руками" администратора ИБ компании-заказчика выполнить все "ключевые" завершающие фазы построения ПИБ: назначение и организация хранения паролей доступа, генерация секретных ключей, программирование устройств аутентификации пользователей, контроль окончательной настойки МЭ и т.д. Такой подход, а также качественное документирование возможностей ПИБ, позволит вам обеспечить надежное функционирование этого нового и необходимого элемента современной КС.