КРУГОВАЯ ОБОРОНА ВАШЕЙ ИНФОРМАЦИИ

Роман Кобцев,
ОАО «ЭЛВИС-ПЛЮС»

"БИЗНЕС-ФОРУМ IT", №9, 2003 г.

Сегодня словами о необходимости защиты информации уже никого не удивишь. И темпы роста преступлений в сфере высоких технологий уже не являются не только какой-либо сенсацией, но и вообще новостью

«Оборона должна быть устойчивой и активной, способной
противостоять ударам всех видов оружия»

Боевой устав сухопутных войск ВС РФ

Не хочу загружать вас большими массивами статистических данных, но без каких-то цифр все же не обойтись. Например, по информации Cnews.ru, только за период 2000-2001 гг. ущерб от сетевых мошенничеств увеличился без малого вдвое: если в 2000 г. он составил 2,4 млрд. долл., то в 2001 г. – уже 4,3 млрд. долл. Число «инцидентов» также растет примерно на 100% в год, что отмечают практически все аналитики.

Темпы, что и говорить, впечатляющие, и чтобы не тратить напрасно время на разговоры о необходимости повышения информационной безопасности, перейдем сразу к вопросу о том, как это делать.

Долгое время обеспечение безопасности информации сводилось к тому, что просто ставили «человека с ружьем» у того помещения, где она хранилась, и все проблемы были решены. Затем этого стало недостаточно, и начало превалировать мнение, что информацию нужно еще и шифровать. Такой защиты снова хватило надолго, но современный уровень развития технологий требует всестороннего обеспечения безопасности информации, и в настоящее время число компаний, называющих свои решения в этой области комплексными, растет.

При этом здесь, как и везде, сколько людей, столько и мнений о том, как ее обеспечить, и, что интересно, все эти мнения имеют право на существование – ведь академического определения понятия «комплексная защита информации» на сегодняшний день просто не существует. Подход к построению комплексной системы информационной безопасности (КСИБ), который представлен далее, конечно, тоже не претендует на звание эталона, однако он уже успел показать себя на практике. Суть его заключается в том, что под комплексной защитой информации понимается не комплекс разнообразных средств защиты, а комплекс мер (мероприятий), направленных на создание надежной системы безопасности информации. Вопрос лишь в том, какими должны быть эти меры.

Системный подход – всему голова

Выстраивание информационной безопасности компании должно базироваться на системном подходе, так как только он позволяет сформировать комплекс мероприятий по парированию угроз безопасности - начиная с анализа состояния объекта и заканчивая выдачей гарантии качества принятых мер. И не стоит считать это бесполезной «тягомотиной», ведь как сказал Гельвеций, «чтобы удивиться, достаточно одной минуты. Чтобы сделать удивительную вещь, нужны многие годы».

Процесс создания КСИБ можно разделить на четыре стадии. Первая – это анализ текущего состояния безопасности компании: сначала оцениваются масштабы «бедствия» и определяется, что конкретно нужно защищать на конкретных объектах (в том числе, требуется ли там вообще защищать информацию). На данном этапе определяется объект защиты, моделируются информационная система и угрозы безопасности информации. Следует сказать, что данный этап – один из самых важных, ибо оценка угроз и их источников – залог того, что потенциальную катастрофу удастся предотвратить.

После того, как стало понятно, в каком состоянии находится информационная система и какие угрозы безопасности информационных ресурсов актуальны для данного объекта, необходимо выработать некую концептуальную систему взглядов на решение проблемы. Поэтому следующая стадия – определение целей и постановка задач защиты, выбор уровней и формулирование технических требований к защищенности и средствам защиты. Здесь же осуществляется категорирование защищаемых объектов по степени важности,

определяются методы и способы ликвидации последствий возможных атак, определяется оптимальное соотношение используемых методов защиты. И только после выработки всей этой целостной системы взглядов можно приступать непосредственно к третьему этапу – созданию системы информационной безопасности.

На этой стадии идет проектирование системы, выбор партнеров и субподрядчиков, аппаратных и программных средств защиты, реализация технических требований и разного рода организационных мероприятий.

Завершают стадию подтверждения эффективности принятых мер защиты (т. е. оценка результатов реализации системы безопасности) страхование ответственности производителя, периодические плановые и внезапные проверки и другие меры.

Что защищаем?

Построение КСИБ не случайно начинается с выбора объекта защиты. Давайте сразу определимся в споре, что следует защищать: автоматизированную систему или информацию, обрабатываемую в этой системе?

Если вы собираетесь защищать автоматизированную систему, то проблема решается очень просто, – поставим ранее уже упомянутого человека с ружьем, и можно спать спокойно. Но если вы считаете, что защищать нужно обрабатываемую информацию, здесь так просто уже не отделаешься: ведь информация – это не единицы и нули в компьютере. Это гораздо более широкое понятие, и информация может быть потеряна не только в результате действий хакеров: её, как и сотни лет назад, можно прочитать или услышать, переписать на бумагу или попросту пересказать, и хакеры тут будут совершенно ни при чем.

Человеческий фактор по-прежнему главенствующий в деле информационной безопасности, и чтобы похитить информацию, порой не нужно не только разбираться в информационных технологиях, но и вообще иметь какое-либо образование. Если, например, бандит с образованием три класса положит вашему системному администратору в его собственном доме утюг на спину, то можно только гадать, что произойдет быстрее, – утюг нагреется или администратор сам выложит все ваши секреты и еще тесемочкой их перевяжет… Поэтому мы считаем, что защищать следует именно информацию, и в некоторых случаях для этого могут вообще не понадобиться компьютерные технологии (достаточно только организационных мероприятий).

Ну а если уж речь идет о защите информационных ресурсов, то из них нужно выбрать те, что содержат сведения ограниченного доступа. Что это за сведения, определить должен собственник информации: у кого-то это исходные коды нового программного продукта, у кого-то – счета «черной» бухгалтерии, у кого-то – тайная фотография постельной сцены или еще что-то, важное для него, и цель защиты – «исключить нанесение материального, морального и иного ущерба собственникам информации в результате нарушения ее целостности, доступности и конфиденциальности».

Этот подход имеет существенное преимущество перед другими. Во-первых, цель мероприятий по защите информации - вполне конкретная и понятная высшему руководству, которому, как правило, недосуг вникать в поток технической мысли, выливаемый ему на голову руководителем службы безопасности информации в попытках обосновать необходимость построения «той самой» системы защиты. Во-вторых, он привязывает сферу защиты информации к такому атрибуту нашей жизни, как закон, и это позволяет собственнику в случае, если информация у него все-таки пострадает, требовать ответа за это в рамках правовой системы государства[1].

Средство соотнесения затрат с «размерами кошелька»

Особое внимание следует уделить оценке угроз безопасности информации – ведь, как сказал когда-то Виссарион Белинский, «найти причину зла – почти то же, что найти лекарство против него».

---

1 Имейте в виду, что сама по себе атака на информационные ресурсы, не приведшая ни к каким последствиям, преступлением не является, и привлечь к ответственности за нее нельзя, на что не раз обращалось внимание на различных конференциях, в том числе представителями подразделений МВД по борьбе с преступлениями в сфере высоких технологий.

Другая состоит в том, что если перевести цель защиты информации из юридической плоскости в практическую, то ее можно сформулировать так: не допустить или ослабить ущерб от атак на информационные ресурсы компании, осуществляемых через уязвимости в системе безопасности. А это значит, что при реализации данной системы необходимо в первую очередь максимально полно определить угрозы безопасности информации и уязвимости информационной системы, причем, как уже указывалось, конкретно по каждому объекту.

В принципе, угроз, способных нанести ущерб собственнику информации, не так уж и много: это хищение информации, ее утрата, блокирование, уничтожение и модификация, а также отрицание подлинности достоверной информации и навязывание ложной. При этом для предотвращения подобных угроз существует «джентльменский» набор методов: правовые, организационные, технические, инженерно-технические и программно-аппаратные.

Следует заметить, что тщательный анализ угроз позволяет оставить в стороне разговоры о необходимости построения «абсолютной» системы безопасности информации, а заняться оптимизацией системы и, соответственно, затрат на нее, соотнеся их с «размерами кошелька». Такая оптимизация может вестись за счет экономии на мерах безопасности от наименее актуальных или реальных угроз (к примеру, если защищаемый объект находится в местности, где последнее землетрясение было пару миллионов лет назад, то можно не особо беспокоиться об обеспечении дополнительной защиты серверной комнаты от разрушения в результате землетрясения).

Как построить неприступную стену

КСИБ можно представить себе в виде некой стены, которая со стороны выглядит неприступным монолитом. Однако при ближайшем рассмотрении можно увидеть, что она состоит из множества кирпичиков-элементов. Что же это за элементы?

КСИБ должна строиться не просто по многоуровневому принципу, а в виде нескольких последовательных рубежей - таким образом, чтобы наиболее важная с точки зрения безопасности зона (наиболее сохраняемые секреты) находилась в центре и была защищена максимальным числом «слоев» безопасности. Это значит, что КСИБ должна обеспечивать безопасность информации на всех уровнях: физическом, технологическом, пользовательском, сетевом и канальном.

На физическом уровне безопасность реализуется физической защитой программных и аппаратных средств с использованием технических средств охраны и наблюдения. На технологическом уровне она может быть достигнута как результат использования доверенного ПО[2] и надежного оборудования (от его надежности зависит доступность информации), защиты программной и аппаратной платформ средствами акустической и виброакустической защиты информации, применения инструментов защиты аппаратных средств от побочных электромагнитных излучений и наводок (ПЭМИН) и другого специального технического инструментария.

Безопасность информации на пользовательском уровне – это защита индивидуальной рабочей среды пользователя, что реализуется путем идентификации и аутентификации пользователей, а также разграничения их полномочий на доступ к информационным ресурсам.

Безопасность информации на сетевом уровне достигается как индивидуальной защитой сегментов локальных сетей[3], так и внешнего периметра сети компании от атак через Интернет. Для защиты здесь используются фильтрация информации, межсетевые экраны[4], доверенная маршрутизация[5] и VPN[6].

---

2 В соответствии с ГОСТ ИСО 7498-99, доверительная функциональность – это функционирование системы, которое воспринимается правильным с точки зрения некоторого критерия, отвечающего стратегии защиты. Таким образом, доверенное ПО – это проверенное программное обеспечение, функции которого (в том числе и защитные) протестированы и имеют документальное подтверждение успешности тестирования.

3 Эти сегменты могут быть сформированы исходя из таких признаков, как общая для группы сотрудников «функциональность» или «территориальность», а также в зависимости от уровня ценности для компании обрабатываемой информации.

4 Межсетевой экран – средство контроля за информацией, поступающей в автоматизированную систему и/или выходящую из нее, обеспечивающее защиту посредством фильтрации информации.

Безопасность на канальном уровне достигается шифрованием либо преобразованием[7] трафика с удаленными пользователями и применением электронно-цифровой подписи, а также использованием доверенных каналов связи[8].

Предположим, все это реализовано. Можно ли тогда сказать, что мы получили комплексную систему информационной безопасности? Едва ли – это пока всего лишь разрозненные элементы системы, как горка кирпичей, сваленная в кучу перед началом строительства стены: с одной стороны, каждый кирпич по-своему хорош – он прочен и совершенен и обеспечивает какую-то преграду, однако, чтобы построить из этих кирпичей стену, нужно сложить их определенным образом и скрепить между собой цементом.

То, что позволяет все эти разрозненные «элементы-кирпичи» сложить в том порядке, который обеспечит максимальную прочность применительно к построению «стены» безопасности информации, – это системный подход. А сцементировать нашу «комплексную стену» должно централизованное управление безопасностью – именно оно позволяет собрать все применяемые продукты и подсистемы, поддерживающие и дополняющие функциональность друг друга, в единую комплексную архитектуру безопасности, обеспечивающую выполнение общей задачи – защиты информации. Но разговор об управлении безопасностью – это тема для отдельной статьи…

С другими статьями, посвященным вопросам информационной безопасности, Вы можете ознакомиться на сайте «ЭЛВИС-ПЛЮС»: http://www.elvis.ru/informatorium.shtml

---

5 Процесс организации передачи информации через снабженные доверенным ПО устройства маршрутизации (концентраторы, маршрутизаторы, ключи, разветвители и т. п.), гарантирующие прохождение трафика от одного доверенного пользователя к другому и исключающие возможность его несанкционированного перенаправления.

6 От английского Virtual Private Network (виртуальная частная сеть). VPN-устройства – средства построения защищенной сети, обеспечивающие безопасный удаленный доступ к информационным ресурсам локальных сетей со стороны мобильных или удаленных пользователей, безопасное объединение вычислительных сетей территориально распределенных подразделений компании и защиту информации, передаваемой по каналам связи в рамках одной вычислительной сети.

7 В принципе, это более широкое понятие, чем «криптография», предполагающее возможность использования также математических или иных преобразований информации, например, ее скремблирование (перестановка элементов сообщения с целью его маскировки), стеганографирование (метод сокрытия текстового файла в мультимедийном формате – картинке, звуковом или даже видеофайле) и т. п. Их применение может быть обусловлено экономическими соображениями и серьезными законодательными ограничениями на использование криптографии.

8 Доверенный канал – механизм передачи информации между VPN-устройствами, обеспечивающий конфиденциальность и целостность передаваемой информации, а также реализующий взаимную аутентификацию VPN-устройств.