Информационная безопасность и интересы бизнеса

А. Березин, ОАО «ЭЛВИС-ПЛЮС»

E-mail: anber@elvis.ru; Тел.: 531-4633

Обсуждение проблемы обеспечения информационной безопасности (ИБ) бизнеса становится все более и более популярной темой в различных «околокомпьютерных» СМИ. Как правило авторы статей изощряются в описании различных решений, анализируют преимущества и недостатки известных продуктов и технологий, описывают новые подходы и методики и т.д. При этом как-то само-собой разумеющимся и потому остающимся за кадром является тезис о том, что данная проблема актуальна и ею безусловно необходимо заниматься. В тени остается вопрос о том, каковы же собственно интересы Бизнеса в решении этой проблемы? Ведь стандартного тезиса о том, что критичная для Бизнеса информация должна быть доступной, целостной и конфиденциальной явно недостаточно, учитывая, что информация - понятие достаточно эфемерное; угрозы безопасности такой информации носят сугубо вероятностный характер (а как известно, пока гром не грянет, мужик не перекрестится, т.е. в данном случае руководство денег не даст), а технические и организационные решения по безопасности стоят очень конкретные, и немалые кстати, деньги!

Видимо, объяснение указанному явлению кроется в том, что обсуждается данная проблема в основном на уровне технических специалистов или специалистов, имеющих явные «технические корни». А как раз на данном уровне проблема осознана, наверное, уже в максимальной степени. Ведь кто, как не системный администратор может знать, что можно сделать с его сетью, если в нее проникнет недружественная личность с вандалистскими наклонностями? Или разрушающий программный код? Или если выйдет из строя какой-то базовый элемент корпоративной информационной системы (КИС)? Технический специалист также хорошо знает, что можно сделать с потоком данных, если его перехватить. И т.д. и т.п. Но с уровня бизнес-управления компанией этих угроз «не видно», поэтому осознание проблемы обеспечения безопасности информации КИС весьма и весьма туманное. Зато вполне осознанны другие категории: зачем тратить деньги на систему, полезность которой для бизнеса далеко не очевидна? Более того, часто можно услышать такой вопрос: А зачем нам вообще нужна информационная безопасность? На этом же нельзя заработать! Или,

говоря языком бизнеса, зачем нам создавать еще один затратный центр? Их у нас и так слишком много! И с этими аргументами достаточно трудно спорить. Особенно, если не иметь контраргументов, понятных Бизнесу. К сожалению, часто российские CIO (или директора по автоматизации; или начальника департамента информационных технологий) таких контраргументов и не имеют, хотя внутренне совершено уверены в необходимости решения данной задачи. В чем же причина?

Начнем с того, что опишем портрет типичного российского CIO. В большинстве случаев это люди с хорошим техническим образованием, большим опытом работы в отделах АСУ, прекрасно разбирающиеся в ИТ, обладающие прекрасной эрудицией в широкой предметной области, которые за годы работы в организации выросли от рядового инженера до CIO. Другими словами, это люди с теми же самыми «техническими корнями», для которых проблема ИБ очень и очень понятна. И решение проблемы они, как правило, видят тоже исключительно на техническом уровне в виде создание технической системы ИБ с набором стандартных элементов: антивирусы, межсетевые экраны, VPN, сервера доступа и др. Но язык Техники не понятен Бизнесу, равно как и язык Бизнеса далек от языка Техники. А потому для обоснования перед руководством необходимости потратить деньги на безопасность оперировать чисто техническими понятиями совершенно бесперспективно. Вас все равно не поймут! И выхода из такой ситуации для CIO всего два: либо научить технике директора, либо самому освоить язык бизнеса и на нем попробовать убедить руководство в своей безусловной правоте. Как это не странно, первый путь очень даже популярен, хотя в данном контексте хорошо видна его абсурдность.

Итак, что же нужно сделать CIO, чтобы убедить руководство в необходимости воспринимать информационную безопасность как один из корпоративных бизнес-процессов? Или, другими словами, как представить ИБ с точки зрения бизнеса?

Начнем, так сказать, «от печки», т.е. попробуем определить бизнес-задачу ИБ. Одним из основных двигателей рынка автоматизации бизнеса является стремление самого бизнеса стать более эффективным за счет использования современных ИТ. Такое стремление понятно: не так уж много осталось реальных механизмов повышения конкурентоспособности, и все они в основном уже исчерпаны, а ИТ предлагают поистине неограниченные возможности. В том, что в автоматизации бизнеса заложен огромный потенциал для его динамического развития не сомневается сегодня, наверное, уже никто. Для этого достаточно сравнить эффективность и оперативность

работы, например, корпоративной электронной почты с толпой бегающих по коридорам секретарш, качество и сроки разработки сложных технических систем с помощью CAD/CAM/CAE-систем и с помощью традиционного кульмана и др. Можно сказать, что бизнес-задача КИС, как и любой другой технической системы, состоит в том, чтобы упростить, ускорить или сделать более удобными ранее рутинные, и потому медленные и изобилующие ошибками бизнес-процессы. Или, если говорить более строго, любая действующая в интересах бизнеса техническая система в принципе должна предоставлять бизнесу какой-то тип сервиса. Такой сервис может быть самым разнообразным: доменная печь «оказывает услуги» по выплавке стали, транспортный цех - по транспортировке грузов, заводская столовая - по питанию сотрудников и т.д. Также и КИС, будучи сугубо технической системой, оказывает бизнесу свой тип сервиса – в данном случае сервис ИНФОРМАЦИОННЫЙ. И этот сервис заключается в конечном итоге в предоставлении Бизнесу необходимой ему ДЛЯ ПРИНЯТИЯ РЕШЕНИЙ Информации нужного качества, в нужное время и в нужном месте! Т.е. в конечном итоге Информации ДЛЯ УПРАВЛЕНИЯ самим бизнесом!

По сути Информация постепенно становится одним из ключевых элементов бизнеса! Ведь что такое Информация с точки зрения Бизнеса? По сути - это не что иное как некий набор формализованных (в смысле структурированных, разложенных по полочкам и имеющих средства для поиска и представления) знаний Бизнеса О САМОМ СЕБЕ! Причем в данном случае под Информацией можно понимать не только какие-то статичные информационные ресурсы, например, бухгалтерский баланс за прошедший год или текущие настройки какого-то оборудования, но и динамические информационные процессы обработки знаний в виде запрограммированной бизнес-логики работы компании в среде таких популярных приложений как электронный документооборот, ERP, CRM, службы каталогов и др.

Времена Генри Форда, когда управляющий компанией сам привинчивал гайки на конвейере, давно ушли в лету. Сегодня высшее руководство любой компании по существу имеет дело ТОЛЬКО с информацией, на основе которой оно и принимает решения. Понятно, что эту самую информацию готовят множество нижестоящих слоев достаточной сложной пирамиды, которая называется современным предприятием. И что нижние слои этой пирамиды вообще могут не иметь понятия о том, что они производят не только какую-то продукцию или услугу, но и Информацию для руководства. По нашему мнению, глубинный смысл автоматизации бизнеса и заключается как раз в том, чтобы ускорить и упорядочить информационные потоки

между слоями этой пирамиды и представить на самый верх только самую необходимую, достоверную и структурированную в удобной для принятия решения форме Информацию!
Заметим, Информацию ДОСТОВЕРНУЮ! Отсюда можно заключить, что ключевой бизнес-задачей корпоративной системы ИБ является обеспечение гарантий достоверности информации, или, говоря другими словами, гарантий ДОВЕРИТЕЛЬНОСТИ информационного сервиса КИС!

А теперь попробуем провести следующий виртуальный эксперимент. Давайте сначала спросим Бизнес: Готов ли он потратить, скажем, сто тысяч долларов на закупку, например, пяти межсетевых экранов и ста лицензий на антивирусное ПО? А потом зададим тот же самый вопрос по-другому: А готов ли Бизнес потратить сто тысяч долларов на защиту информации о самом себе и на защиту сервиса, на котором основано управление компанией? Скорей всего ответ в первом случае прогнозируем: либо традиционное для России «денег нет», либо по-одесски вопросом на вопрос: А зачем? Во втором случае вариации ответов пошире: В какие сроки управимся? А где ты раньше был? И даже: Почему так мало? Разве мой бизнес столько стоит?
Но будет и вопрос, который любой нормальный Бизнес просто обязан будет задать: А почему именно сто тысяч? А не пятьдесят, или, скажем, не четыреста семьдесят две? И в таком случае наш уважаемый CIO должен быть готов дать понятый Бизнесу ответ, аргументированный необходимыми экономическими выкладками. Т.е. по сути представить обоснование стоимости системы ИБ для Бизнеса.
Такой анализ, безусловно, возможно провести. Внимательный российский CIO наверное уже заметил, что в последнее время в печати все чаще и чаще начинают возникать новые для ИБ темы: анализ угроз ИБ, анализ информационных рисков, оценка совокупной стоимости владения системой безопасности, оценка возврата инвестиций от такой системы и т.д. Все это в виде метрики безопасности представляет собой некий экономический инструментарий, преломленный в область ИБ, который и позволяет ответить на вопрос: А почему сто тысяч? И еще это яркий показатель того, что наиболее «продвинутые» CIO уже пытаются на него ответить.
Автор не ставит своей целью даже кратко описать этот инструментарий, поскольку, во-первых, рамки журнальной статьи не позволяют обсудить эту тему достаточно серьезно, а во-вторых, заинтересованному CIO сегодня несложно найти специализированную информацию на эту тему. В том числе и на русском языке. Кроме

того, уже многие российские ИТ-компании успешно предлагают консалтинговые услуги по оценке метрики безопасности. Однако, хочется обратить внимание CIO на несколько очень важных моментов, которые необходимо иметь в виду при знакомстве с данным инструментарием или при проведении переговоров с консалтинговыми компаниями. Но для этого нам придется несколько отвлечься от намеченной темы.

Попробуем найти достаточно близкую аналогию с системами ИБ в области нашей повседневной жизни. Возьмем, например, «старый добрый» сейф. И представим типичную для большинства компаний ситуацию: главному бухгалтеру необходимо хранить у себя в кабинете крупные суммы наличных денег или каких-то других ценностей. В ворах и грабителях у нас, к сожалению, дефицита нет, поэтому главбух разумно желает эти ценности как-то защитить и автоматически приходит к идее поставить в кабинете сейф. Знакомо? Еще как! Далее гдавбух идет с директору и просит его выделить деньги на покупку сейфа. Трудно представить себе ситуацию, когда директор вдруг скажет, что на это денег нет. Скорей всего это просто не придет ему в голову, ибо деньги должны лежать в сейфе – это аксиома! Поэтому директор деньги выделит. Вопрос: сколько? Опять же трудно представить себе ситуацию, когда директор попросит главбуха подготовить экономическое обоснование оптимальной стоимости сейфа, провести оценку возврата инвестиций от покупки сейфа и т.д. Но мы предположим, что все-таки попросит. И главбух в глубокой задумчивости начнет размышлять: 1) по законам арифметики потенциальный ущерб от отсутствия сейфа в конторе равен той сумме, которую могут выкрасть потенциальные воры минус стоимость самого сейфа; 2) если стоимость сейфа еще можно как-то оценить, то как оценить ту сумму, которая потенциально будет лежать в кабинете бухгалтера В ТОТ САМЫЙ ДЕНЬ? А когда наступит ЭТОТ ДЕНЬ? А как объективно оценить, сколько раз случиться ограбление? А может ли случиться такое, что ограбления не случиться и при отсутствие сейфа? И т.д. и т.п. Поэтому, скорей всего, найти правильно обоснование оптимальной стоимости сейфа ему вряд ли удастся и на покупку сейфа, КАК ОБЫЧНО, будет выделено столько денег, сколько покажется разумным на тот момент.

Наконец, сейф куплен, установлен и эксплуатируется. Но, к сожалению, наш главбух оказывается рассеянной личностью и он вводит в код замка сейфа дату своего рождения; или ключ от сейф кладет под газетку на его крышку; или иногда просто забывает его закрывать. И однажды сейф успешно опустошают.

Из такого «лирического» отступления можно сделать три важных для нас наблюдения, которые вкупе условно можно назвать «законами сейфа»:

- в случае наличия в компании каких-либо ощутимых материальных ценностей, их хранение в сейфе воспринимается как безусловный фактор, не требующий обоснования;
- реальное экономическое обоснование оптимальной стоимости сейфа невозможно в принципе, поскольку в принципе невозможно оценить стоимость того, что этот сейф защищает;
- даже установка Суперсейфа не дает гарантий того, что ваши ценности окажутся в целости и сохранности. Может оказаться нерадивый главбух. Или очень «радивый» медвежатник.

Теперь вернемся к ИБ и попробуем провести аналогию с описанным случаем. Итак деньги – это информация, главбух – CIO, бухгалтерия – аналог информационной системы, сейф – система ИБ, воры – хакеры. Не правда-ли – очень похоже? А поскольку аналогия настолько полная, может быть для ИБ справедливы те же выводы, что и к сейфу. Попробуйте сделать их сами!

А теперь настало время вернуться к нашему CIO, который по-прежнему думает о том, как же ему обосновать перед руководством стоимость системы ИБ в сто тысяч долларов. Поначалу он понадеялся было на метрику безопасности, но наши расуждения о сейфе совсем сбили его с толку! И что же теперь делать? Ведь должен же быть выход! И такой выход есть! И даже два!

Первый, назовем его наукообразным, подход, заключается в том, чтобы освоить, а затем и применить на практике необходимый инструментарий получения метрики безопасности, а для этого ОБЯЗАТЕЛЬНО привлечь руководство компании (как ее собственника) к оценке СТОИМОСТИ защищаемой информации. В таком случае от результатов такой оценки будет во многом зависеть деятельность CIO в области ИБ. Если информация не стоит ничего и руководство это ПОДТВЕРДИЛО (!), проблемой ИБ можно вообще не заниматься. Если информация стоит конкретных денег, понятны рамки бюджета системы ИБ. Хотя у автора есть серьезные сомнения, что руководство большинства компаний сможет назвать конкретную сумму, в которую оно оценивает свою бизнес-информацию, данный подход как минимум дает возможность вовлечь руководство компанией в осознание проблем ИБ и заставить его задуматься о реальной стоимости бизнес-информации. Это дорогого стоит, не правда ли!

Второй подход, назовем его примитивным, состоит в следующем: можно вообще ничего не оценивать, если найти тот самый инвариант разумной стоимости сейфа, т.е. системы ИБ. Ведь существуют же такие инварианты в других отраслях, где значимые для бизнеса события носят вероятностный характер. Например, автострахование. Любой владелец автомобиля может годами не страховать своего «железного коня» и реально сэкономить на этом кучу денег. Но однажды въехать в 600-ый и потерять все. А можно, конечно, и не въехать и, соответственно, не потерять. На что многие и надеются. Однако во всех цивилизованных странах мира уже на уровне социальной этики принято страховать свои автомобили и жить спокойно. И существует некоторая общая оценка разумной стоимости этой услуги на рынке автострахования – 5-15% от рыночной стоимости авто в зависимости от локальных условий его эксплуатации (культура вождения, интенсивность движения, состояние дорог и т.д.).

Полная аналогия с ИБ. Можно вообще не заниматься ИБ и не исключен вариант, что такой риск себя вполне оправдает. А можно вложить в ИБ кучу денег, и все равно останется в системе ма-а-а-ленькая дырочка, через которую информация будет успешно «утекать». Поэтому цивилизованный мир также нашел некий оптимум, при котором можно чувствовать себя относиться уверенно – стоимость системы ИБ должна составлять 10-20% от стоимости КИС в зависимости от уровня конфиденциальности информации. Это и есть та самая оценка (best practice), с которой CIO может уверенно оперировать. И на вопрос руководства: А почему сто? бодро отвечать: А потому-что на сегодняшний день стоимость нашей КИС составила один миллион долларов!

Второй подход, очевидно, не лишен недостатков. Однозначно не удаться вовлечь руководство в глубокое осознание проблем ИБ. Но зато можно смело прогнозировать объем бюджета на ИБ и хорошо сэкономить на консультантах.

Но и в том и в другом случае грамотному CIO не стоит забывать о третьем «законе сейфа» – даже самая дорогая и безупречно экономически обоснованная система ИБ себя не оправдает, если ее элементы непрофессионально установлены или настроены. Другими словами, если не гарантировано качество системы ИБ. Но это уже отдельная тема, может быть для последующих статей.