УДК 006.034

ОБОСНОВАНИЕ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Минзов Анатолий Степанович[1], Кольер Сергей Михайлович[2]

[1]Доктор технических наук, профессор;
ГОУ ВПО «Международный Университет природы, общества и человека «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: a@minzov.ru.

[2]Аспирант;
ГОУ ВПО «Международный Университет природы, общества и человека «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: sergey@kolier.ru.

Данная работа описывает ряд проблем, возникающих при принятии управленческих решений в сфере обеспечения информационной безопасности (ИБ). В статье показано, что существующие на данный момент стандарты (ГОСТ Р) покрывают область ИБ с точки зрения специалиста по ИБ, но не предоставляют механизмов обоснования выбранных стратегий и необходимых на их реализацию бюджетов. В работе отмечается, что использование различных методов оценки (TCO, ROI, ROISI) так же не может полностью и адекватно отразить ситуацию, поднимаются вопросы о совместном использовании руководящих документов (ГОСТ Р и других) и нескольких методов оценки.

Ключевые слова: информационная безопасность, управленческие решения.

METHODS OF SUBSTANTIATION OF ADMINISTRATIVE DECISIONS IN SPHERE OF INFORMATION SECURITY MAINTENANCE

Minzov Anatoliy[1], Kolier Sergey[2]

[1] Doctor of Science in Engineering, Professor;
Dubna International University of Nature, Society, and Man,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: a@minzov.ru.

[2] Postgraduate student;
Dubna International University of Nature, Society, and Man,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: sergey@kolier.ru.

The given work describes some problems which are encountered during making administrative decisions in sphere of information security maintenance. In this article it is revealed that existing standards (GOST) cover an area of information security in terms of IS-specialist, but do not provide mechanisms to justify the chosen strategy and the need to implement their budgets. It is noted in this paper, that using of different assessment methods (TCO, ROI, ROISI) also could not fully and adequately reflect the situation with IS; also the questions was raised about the joint use of guidance documents (GOST R and others) and several methods for assessing.

Keywords: information security, administrative decisions.

Введение

Организации, их информационные системы и сети все чаще сталкиваются с различными угрозами безопасности, создающими реальную опасность их существованию. Вместе с процессом быстрого развития и непрекращающимся ростом степени сложности информационных технологий (ИТ), а так же увеличением возможных каналов распространения информации возникает целый ряд проблем контроля за информацией. К таким проблемам можно отнести как атаки из внешних источников (различные виды мошенничества, взлома, атаки типа «отказа в обслуживании» и т.д.), так и внутренние («инсайдерские») атаки, т.е. несанкционированные действия сотрудников собственной организации, утечки информации, разведывательная деятельность конкурентов и т.п. Как следствие реализации подобных ситуаций – возможный ущерб, связанный с полной или частичной потерей, хищением информации или затратами на восстановление информационной системы организации. Кроме того, хищение критически важной для компании информации может принести ей значительные убытки или даже свести на нет возможность её существования, если украденные данные становятся доступны конкурентным структурам.

Информация, поддерживающие её процессы, информационные системы и сетевая инфраструктура давно стали существенными активами организации, активами, которые имеют ценность и, следовательно, должны быть защищены надлежащим образом. Кроме того, конфиденциальность, целостность и доступность информации существенно способствуют обеспечению конкурентоспособности, ликвидности, доходности, соответствия законодательству и деловой репутации организации.

Начавшийся в 2008-м году глобальный экономический кризис сказался на финансовой политике многих организаций и привёл к пересмотру всего перечня затрат, в том числе и бюджетов на ИТ. Половина компаний приостановили часть своих ИТ-проектов, более 60% ИТ-директоров заявили о сокращении ИТ-бюджета на 2009-й год, причём 39% отметили о сокращении на 20% и более [1, 2]. Однако глобальный экономический кризис не сказался на злонамеренных лицах, желания которых по меньшей мере остались на прежнем уровне, а в некоторых случаях возросли. Связанные с криминалом риски ИБ растут, появляются новые виды угроз, а, значит, им должны оказываться адекватные меры защиты и противодействия. Проблема защиты информации остаётся открытой в любые – благоприятные или кризисные – времена и поднимает множество сопутствующих вопросов:

- Как защитить информацию от несанкционированного доступа?
- Как защитить информацию от порчи, кражи или утечки?
- Что важнее для компании: в первую очередь защитить информацию от внешних или внутренних угроз? Если необходимо обеспечение ИБ на всех возможных направлениях угроз, то, в таком случае, какие конкретно меры нужно предпринимать и какие именно финансовые вложения для этого требуются?
- Почему стоит выбрать определённую стратегию обеспечения ИБ из нескольких альтернатив?

Это лишь небольшая часть вопросов ИБ, которые остаются актуальными всегда, стало быть, обеспечение ИБ не может и не должно забываться организациями как класс задач, а, напротив, должно превращаться в конкурентное преимущество.

Информационная безопасность. Два взгляда на проблему

Идеальным решением является решение задачи обеспечения ИБ (по каждому i-му риску) с минимальными финансовыми затратами Z при максимальной эффективности E:

$$\begin{cases} Z = \sum_i Zi \to \min \\ E = \sum_i Ei \to \max \end{cases}.$$

К сожалению, подобное решение едва ли осуществимо и поэтому зачастую приходится искать компромисс между затратами на ИБ и остающимися угрозами. Каким должен быть механизм поиска этого компромисса?

В настоящее время не существует классификации методик и моделей экономического обоснования выбора тех или иных решений по организации ИБ. Основная причина заключается в том, что существующие подходы к защите информации основаны на ряде стандартов (ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 13335 и других), в основу которых положены рекомендации или последовательности работ по проведению аудита информационной безопасности, разработки модели угроз, определение мероприятий по защите от них и организация внедрения этих мероприятий. Экономическая целесообразность организационных действий и технических решений во внимание не берётся. В случае появления требования по сохранению государственной тайны подобный подход вполне оправдан, особенно, когда речь идёт об оборонных или военно-промышленных предприятиях, так как чаще всего финансирование на информационную безопасность идёт за счёт бюджета. В случаях, не связанных с государственной тайной, оборонной промышленностью и прочих подобных ситуациях, жёсткое следование данным подходам не всегда имеет практический смысл.

Если поднимается вопрос о непрерывном функционировании бизнеса, то, безусловно, необходимо описать все бизнес-процессы и определить все активы, а также сведения, представляющие для организации интеллектуальную собственность – это будет являться отправной точкой для дальнейших работ по обеспечению информационной безопасности. ГОСТ Р ИСО/МЭК 27001 в первых своих строках предполагает использование процессного подхода для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения системы ИБ [7]. В отношении тех же действий ГОСТ Р ИСО/МЭК 17999 дополняет: «Организация должна определить свои требования к информационной безопасности с учётом следующих трех факторов:

- во-первых, оценка рисков организации. Посредством оценки рисков происходит выявление угроз активам организации, оценка уязвимости соответствующих активов и вероятности возникновения угроз, а также оценка возможных последствий;
- во-вторых, определить юридические, законодательные, регулирующие и договорные требования, которым должны удовлетворять организация, ее торговые партнёры, подрядчики и поставщики услуг;
- в-третьих, определить специфический набор принципов, целей и требований, разработанных организацией в отношении обработки информации» [6].

Нет никаких сомнений в правильности и необходимости первых двух требований: результаты оценки рисков помогут в определении конкретных мер и приоритетов в области управления рисками, связанными с ИБ, а также внедрению мероприятий по управлению ИБ с целью минимизации этих рисков. Кроме того, оценка и анализ риска призваны объяснить адекватность затрат на внедрение решений ИБ. Второе требование вполне очевидно – все процессы в организации должны соответствовать законодательным и нормативным требованиям. Однако с третьим требованием начинаются трудности. Действительно, в зависимости от сферы деятельности у каждой конкретной организации найдётся ряд специфических аспектов работы. Как максимально правильно оценить эти специфические стороны, а также связанные с ними риски? Каким образом реализовать их эффективную защиту? К сожалению, ответы на эти вопросы стандарт не даёт.

ГОСТ Р ИСО/МЭК 17999 отмечает необходимость постоянной повторяющейся оценки и отслеживания рисков информационной безопасности «для того, чтобы охватить различные подразделения организации или отдельные информационные системы и учесть:

- изменения требований и приоритетов бизнеса;
- появление новых угроз и уязвимостей;
- снижение эффективности существующих мероприятий по управлению информационной безопасностью» [7].

Каким образом реализовать это верно и максимально эффективно, а также как подтвердить, что полученные результаты адекватно отражают положение вещей и не являются интуитивным умозаключением? Эти вопросы также пока остаются без ответа. Это подтверждается результатами исследований некоторых компаний, которые заключают, что «...российские компании готовы вводить организационные меры для части бизнес-процессов и активов, но пока не готовы тратить деньги на пол-

ноценную систему управления информационной безопасностью (СУИБ), так как не могут пока оценить её экономическую эффективность» [3]. Действительно, в существующем сложном окружении непросто посчитать последствия инцидентов ИБ, которые не произошли или были предотвращены. Сложно, если вообще возможно, посчитать вероятные финансовые потери, которых удалось избежать, а, значит, сложно принять решение о вложении немалых сумм в ИБ, которое нужно сделать сейчас, и о результатах которых заранее узнать невозможно. Кроме того, сфера ИБ обладает одной очень важной отличительной особенностью: если информационная безопасность функционирует достаточно эффективно, то подобные обстоятельства создают обратную связь со знаком минус. Складывается ситуация, в которой с повышением эффективности мероприятий по ИБ уменьшается количество инцидентов и появляется вполне закономерный вопрос «почему?». Вне зависимости ответа на этот вопрос (будь то «общее уменьшение количества инцидентов, «были приняты хорошие меры ИБ», «служба ИБ отлично справляется со своими обязанностями» или что-то ещё) первый очевидный вывод может быть следующим: зачем вкладывать дополнительные средства в ИБ, когда дела обстоят неплохо? Конечно, это очень обманчивая ситуация, но в ней руководителю отдела ИБ потребуются действительно убедительные доводы, чтобы обосновать своему руководству необходимость дальнейших трат.

К сожалению, пока не существует единых организационных решений по взаимодействию служб ИБ и экономических подразделений предприятий. Решение задач обеспечения ИБ и обоснование сопутствующих затрат выглядят по-разному для специалистов разного профиля.

Лица, принимающие решение, в т.ч. по бюджетам (директор, …)	Специалист по ИБ
- Защита информационных ресурсов становится важной задачей бизнеса, принятие тех или иных решений может входить в сферу ответственности руководителей подразделений и бизнеса в целом. - Зачастую менеджмент не разбирается в тонкостях (в т.ч. технических) используемых технологий. - Выбор определенной стратегии обеспечения безопасности не может быть отделён от вопроса о затратах, необходимых для её достижения. Затраты должны быть понятным образом обоснованы. - Менеджмент понимает привычные бизнесу оценки: прямые и косвенные затраты, угрозы и риски, а так же возможность их возникновения и величина ущерба, методы оценок типа ROI, TCO и т.д.	- Защита информационных ресурсов – это функция службы безопасности. - Выбор определённой стратегии обеспечения безопасности и её финансирование основываются, прежде всего, на основании оценки перечня активов организации и анализа связанных с ними угроз и рисков. - В основе оценки рисков и возможного ущерба лежит критерий $Ri = U_i \cdot P_i$, где U_i – величина ущерба от реализации i-го риска, P_i – вероятность его реализации. - Общепринятые экономические методы оценки и обоснования затрат в сфере ИБ как правило не могут быть применены.

Несколько лет назад были предприняты попытки отнести затраты сферы ИБ в категорию инвестиционных затрат. По аналогии с известным и понятным показателем ROI (Return On Investment; прибыль, окупаемость инвестиций), обозначающим отношение увеличения инвестиций (чистой прибыли) к объёму первоначальных инвестиций, была создана модель ROISI (Return on Information Security Investment; прибыль, окупаемость инвестиций в безопасность), которая призвана посчитать прибыль от вложения в ИБ [8]. Ключевое слово в ROI – прибыль. Другими словами, сам ROI позволяет посчитать, сколько прибыли приносит единица капитала, вложенная в бизнес, ведь инвестиции (по определению) порождают прибыль (конечно, в случае их успешности).

В случае с безопасностью ситуация обстоит сложнее: потраченные деньги не создают новые деньги, прибыли как таковой нет и получить её, вообще говоря, невозможно. Очевидны только прямые и косвенные затраты на обеспечение ИБ. Более того, говорить об «инвестициях» относительно ИБ – значит неверно истолковывать сам термин и его понимание в финансовых сферах. Занятия ИБ предполагают исключительно затраты на соответствие законодательным и прочим требованиям, а

также на предотвращение вероятных финансовых, имиджевых и прочих потерь от тех или иных инцидентов. Результатом таких затрат в лучшем случае станет экономия, и модель ROISI может быть применена для её описания, но буквальное соотнесение названия модели с фактическим её содержанием и получаемым результатом даёт некорректную оценку и вводит в заблуждение.

Другая методика, дополнительно использующаяся при расчете бюджетов, – это TCO (Total Cost of Ownership, совокупная стоимость владения) – методика, разработанная аналитической компанией Gartner Group в 1987 г. и предназначенная для определения затрат (в том числе и на информационные системы), рассчитывающихся на всех этапах жизненного цикла системы. Применительно к сфере информационной безопасности TCO может помочь оценить все расходы предприятия по внедрению (модернизации) и эксплуатации системы ИБ. Однако, TCO не может показать эффективность принятых мер и рассчитать затраты в случаях чрезвычайных ситуаций. Подобная оценка будет полезна руководителю, чтобы получить представление о тратах на проект, но не сможет объяснить и обосновать необходимость и эффективность этих трат и потому может играть определённую позитивную роль на начальных этапах планирования ИБ.

Метод	Применимость метода для разных компетенций, возможные варианты	
	Лица, принимающие решения, в т.ч. по бюджетам (директор, …)	Специалист по ИБ
TCO	Может быть полезен для первоначальной оценки совокупной стоимости проекта. Не может обосновать эффективность, но может быть сравнительной характеристикой между несколькими поставщиками одинакового перечня услуг.	Не показывает эффективность проекта, концентрация на стоимости внедрения/модернизации и поддержке. В случае, если специалист по ИБ не имеет представления о возможных размерах бюджетов, то для него этот метод фактически теряет всякий смысл.
ROI	Не может быть применен.	Не может быть применен.
ROISI	Может показать некоторый экономический эффект (экономию средств в будущем) от внедрения.	Может использоваться для демонстрации частичного эффекта от внедрения проекта.

Заключение

Как мы видим, складывается ситуация, когда специалисты по ИБ могут предложить конкретные меры, стоящие конкретных денег, но не имеют возможности привести необходимые основания, дающие руководству ответ на вопрос «Почему должна быть именно такая стратегия, а бюджет должен иметь именно такой размер?».

TCO даёт руководителю представление о стоимости внедрения проекта, прямых и косвенных затратах, показывает, во сколько обойдётся сопровождение решения в будущем. Также оценка TCO может помочь при выборе поставщика услуг по ИБ, т.е. провести сравнение подобных оценок от разных поставщиков на один и тот же проект. Для специалиста по ИБ TCO в чистом виде, вообще говоря, пользы не несёт, т.к. финансовая составляющая его интересует в меньшей степени, тогда как эффективность проекта по ИБ, которую TCO как раз предоставить не может, – интересует в большей степени.

ROI в первоначальном виде не может быть применён в проектах по ИБ, т.к. ни о каких возвратах и тем более прибылях в реализации подобных проектов речь не идёт. Модификация ROISI скорее является методом, способным показать некоторую «экономию средств» от внедрения в будущем. По-

лезна ли эта оценка? Да, безусловно. Доказывает ли она эффективность принятого решения или оценивает его с точки зрения оптимальности? Увы, нет.

Поскольку стандартов, позволяющих оценить ИБ с экономической точки зрения, до сих пор нет, любой из существующих методов имеет право быть рассмотренным для выяснения его применимости, положительных и отрицательных сторон. Возможно, ситуацию улучшит совокупное использование методов TCO, ROI (ROISI) или дополнительное рассмотрение вложения финансов в обеспечение информационной безопасности бизнеса с точки зрения оплаты своеобразной «страховки, страховых взносов на будущее», подобно тому, как страхуются прочие риски. Единственное отличие лишь в том, что подобные «страховые выплаты» снижают вероятность инцидента, но не исключают его полностью и, в случае наступления «страхового случая», компенсаций ожидать не стоит.

Список литературы

1. Зимин К., Костяков С. Сокращение ИТ-бюджетов. [Электронный ресурс]. URL: http://www.iemag.ru/researches/detail.php?ID=18398 (дата обращения: 5.12.2009).
2. Зимин К., Костяков С. Антикризисные меры и резервы сокращения затрат. [Электронный ресурс]. URL: http://www.iemag.ru/researches/detail.php?ID=18424 (дата обращения: 17.01.2010).
3. Рынок информационной безопасности: Эпоха кризиса. Экспертный отчет LETA-IT Company. [Электронный ресурс]. URL: http://www.leta.ru (дата обращения: 13.11.2009).
4. Стандарт ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. – М.: Стандартинформ, 2007.
5. Стандарт ГОСТ Р ИСО/МЭК 13335-3-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий. – М.: Стандартинформ, 2007.
6. Стандарт ГОСТ Р ИСО/МЭК 17799-2006. Информационная технология. Практические правила управления информационной безопасностью. – М.: Стандартинформ, 2006.
7. Стандарт ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы защиты. Системы менеджмента защиты информации. Требования. – М.: Стандартинформ, 2006.
8. Adrian Mizzi. Return on Information Security Investment – The Viability of an Anti Spam Solution in a Wireless Environment. [Электронный ресурс]. URL: http://www.geocities.com/amz/ (дата обращения: 2.12.2009).