Обоснование инвестиций в кибербезопасность

С. А. Петренко

Впервые термин Return on Investment for Security (ROSI) был введен в употребление специалистами в области IT Security после публикации статьи в начале 2002 г. в журнале CIO Magazine «Finally, a Real Return on Security Spending». Примерно в это же время вышло несколько публицистических статьей, посвященных количественным методам оценки затрат на безопасность. Сегодня тема возврата инвестиций (Return on Investment — ROI) в информационные технологии стала темой повышенного интереса для топ-менеджмента многих российских компаний. При этом особое внимание уделяется методам расчета возврата инвестиций в безопасность (Return on Investment for Security — ROSI).

Традиционно обоснования расходов на безопасность были в большинстве своем качественными или «стратегическими», которые доказывали, что без инвестирования в корпоративную систему защиты информации компания упускает более «осязаемые» выгоды. Обоснование расходов на информационную безопасность включало в себя следующие утверждения:

- расходы на безопасность являются составляющей стоимости ведения бизнеса;
- расходы на безопасность родственны расходам на страхование;
- компания не может заниматься электронной коммерцией без обеспечения определенного уровня защиты электронных денежных потоков;
- безопасность является одним из аспектов управления рисками;
- заказчик имеет право подать на компанию в суд, если она отказывается соблюдать минимальные стандарты безопасности (например, защищать конфиденциальную информацию о клиенте);
- нежелание вкладывать денежные средства в безопасность — означает нежелание следовать общим тенденциям развития информационных технологий.

После приведения подобных доводов ни у кого не вызывает сомнений необходимость расходов на требуемый уровень информационной безопасности компании, но вместе с этим появляется необходимость количественного расчета для финансового обоснования инвестиций в корпоративную систему защиты информации. Давайте посмотрим, какие способы обоснования инвестиций в корпоративные системы защиты информации существуют и оправданны на практике.

Метод ожидаемых потерь

Этот подход базируется на том, что вычисляются потери от нарушений политики безопасности, с которыми может столкнуться компания, и эти потери сравниваются с инвестициями в безопасность, направленными на предотвращение нарушений. Метод ожидаемых потерь основан на эмпирическом опыте организаций и сведений о вторжениях, о потерях от вирусов, об отражении сервисных нападений и т. д. Например, нарушения безопасности коммерческих организаций приводят к следующим финансовым потерям:

- при ведении электронной коммерции потери, связанные с простоем и выходом из строя сетевого оборудования;
- нанесение ущерба имиджу и репутации компании;
- оплата сверхурочной работы ИТ-персонала и/или оплата работ подрядчикам, которые занимались восстановлением корпоративной информационной системы;
- оплата консультаций внешних специалистов, которые осуществляли восстановление данных, выполняли ремонт и оказывали юридическую помощь;
- оплата ремонта физических повреждений от виртуальных атак;
- судебные издержки при подаче искового заявления о виртуальных преступлениях и нарушениях политики безопасности.

Чтобы «смягчить» ожидаемые потери, компания должна инвестировать средства в безопасность: сетевые экраны, системы обнаружения вторжений, чтобы предотвратить атаку, антивирусы для обнаружения различных форм вирусов. Если компания решает установить систему информационной безопасности, то ее стоимость обобщенно будет складываться из следующего:

- Единовременные затраты:
  - покупка лицензий антивирусного программного обеспечения, средств Firewall, средств AAA;

- приобретение аппаратных средств;
- возможно оплата консультаций внешнего эксперта в области информационной безопасности.

- Периодические затраты:
  - техническая поддержка и сопровождение;
  - заработная плата ИТ-персонала;
  - затраты на найм необходимых специалистов;
  - затраты на исследование угроз нарушений политики безопасности.

Следует отметить, что нет совершенной системы информационной безопасности. Чтобы определить эффект от внедрения системы ИБ, мы должны вычислить показатель ожидаемых потерь (Annualised Loss Expectancy — ALE). По оценкам экспертов, правильно установленная и настроенная система защиты дает 85 % эффективности в предупреждении или уменьшении потерь от нарушений политики безопасности. Следовательно, финансовая выгода обеспечивается ежегодными сбережениями, которые получает компания при внедрении системы ИБ.

$$AS = ALE \times E - AC,$$

где AS — ежегодные сбережения (Annual Saving), ALE — показатель ожидаемых потерь (Annualised Loss Expectancy), E — эффективность системы защиты (около 85 %), AC — ежегодные затраты на безопасность (Annual Cost).

Метод оценки свойств системы безопасности

Метод оценки свойств системы безопасности (Security Attribute Evaluation Method — SAEM) был разработан в Carnegie Melon University и основан на сравнении различных архитектур систем информационной безопасности для получения стоимостных результатов оценки выгод от внедрения системы ИБ. Методология SAEM заключается в том, чтобы, объединив вероятность события и ранжировав воздействие окружающей среды, предложить различные проекты по информационной безопасности с многовариантным влиянием окружающей среды на относительные затраты.

Недостатком метода является то, что чаще всего безопасность находится вне понимания менеджеров, занимающихся оценкой эффективности, а специалисты по информационной безопасности редко имеют точные данные относительно выгод, приносимых технологией, поэтому приходится полагаться на опыт и интуицию и на их основе принимать

решения. Однако этот метод может быть использован для представления комплекса разнообразных мер по информационной безопасности и для поддержки принятия решения при выборе тех или иных мероприятий.

Анализ дерева ошибок

Нетрадиционным инструментом оценки выгод является метод анализа дерева ошибок (Fault Tree Analysis). Цель применения данного метода — показать, в чем заключаются причины нарушений политики безопасности и какие сглаживающие контрмеры могут быть применены. Дерево ошибок — это графическое средство, которое позволяет свести всю систему возможных нарушений к логическим отношениям «и»-«или» компонентов этой системы. Если доступны данные по нормам отказа критических компонентов системы, то дерево ошибок позволяет определить ожидаемую вероятность отказа всей системы.

Применяя этот метод к системам информационной безопасности, мы можем произвести дерево с причинно-следственными отношениями между атаками на систему и нарушениями системы. Использование контрмер по предотвращению нарушений позволяет уменьшить ответвления дерева и, таким образом, может быть определен эффект от внедрения системы ИБ на сравнении «двух деревьев» с использованием контрмер и без.

Важно заметить, что этот метод базируется на двух связанных предположениях: во-первых, что компоненты системы разрушаются случайным образом согласно хорошо известной статистике, во-вторых, на самом низком уровне дерева составляющие отказа независимы друг от друга. Все-таки отказы программного обеспечения системы ИБ неслучайны, и, скорее всего, возникают из-за системных ошибок, и это в большинстве своем влияет на работу других частей системы. Об этом не следует забывать при применении данного метода к системе информационной безопасности.

В настоящее время этот метод еще недостаточно адаптирован к области информационной безопасности и требует дальнейшего изучения.

Выбор подходящего метода

Принципиальный недостаток приведенных выше методов в том, что они не дают количественной оценки стоимости и выгод от контрмер безопасности, кроме метода ожидаемых потерь, который объединяет выгоду от каждой контрмеры в единый количественный показатель «эффективно-

сти». А с точки зрения системы безопасности, этот показатель интерпретируется как показатель пригодности всей системы защиты, который обычно указан в договоре с поставщиком системы защиты.

Поэтому на практике можно воспользоваться метод оценки целесообразности затрат на систему ИБ. Такой выбор был обусловлен несколькими соображениями — это финансовая ориентированность метода и достаточно полная оценка стоимости различных мер по безопасности и выгод от внедрения. Для того чтобы привести пример оценки мер по обеспечению безопасности, воспользуемся упрощенным вариантом дерева ошибок, так называемой таблицей оценки угроз и рисков (Threat and Risk Assessment — TRA). Использование TRA позволит показать, как на практике получить количественную оценку вероятности событий и возникновения последствий и в дальнейшем использовать эти данные для определении ожидаемых потерь без применения контрмер безопасности.

Методика Return on Investment for Security

В предыдущей статье («Оценка затрат на кибербезопасность») мы определились с методами оценки экономической целесообразности затрат на систему информационной безопасности: расходную часть мы определили с помощью программного продукта «TCO Manager» и получили текущий и целевой показатели совокупной стоимости владения. Сейчас мы оценим доходную часть, объединяя метод ожидаемых потерь с таблицей оценки угроз и риска.

Первым шагом является построение таблицы TRA. Сделаем небольшое отступление и дадим краткое описание контрмер по обеспечению информационной безопасности.

Контрмеры по обеспечению безопасности направлены на достижение следующих эффектов: уменьшение вероятности происхождения инцидента и/или уменьшение последствий, если инцидент все равно случается. Меры, снижающие вероятность, называются профилактическими, а меры, снижающие последствия, называются лечебными. Примеры контрмер обоих типов представлены в табл. 1.

Пусть вероятность происшествия описана семью уровнями от «незначительного» до «экстремального». Определим эти уровни в следующей таблице (табл. 2).

Последствия от нарушения политики безопасности также описаны шестью уровнями от «несущественного» к «критическому» и каждому уровню соответствуют потери в случае ликвидации нарушений, которые определены экспертно специалистами Gartner Group (см. табл. 3).

Таблица 1

Типы контрмер безопасности

Тип контрмеры	Пример
Профилактические	1. Стандарты, процедуры, должностные инструкции. 2. Аудит системы безопасности. 3. Сетевые экраны. 4. Системы обнаружения вторжений. 5. Антивирусы. 6. Средства шифрования. 7. Формирование архивов
Лечебные	1. Резервные режимы работы
Принадлежат обоим типам	1. Планирование непрерывности бизнеса / планирование восстановления бизнеса. 2. Обучение

Теперь рассчитаем показатель ALE для ЗАО «Страхование», используя форму таблицы TRA (табл. 4), в которой сопоставляются вероятности угроз, степень тяжести нарушения и частота событий. Следует отметить, что показатель ALE мы вычисляем согласно формуле:

$$\mathrm{ALE} = f \times L, \qquad (1)$$

где f — частота возникновения потенциальной угрозы, уровень которой определяется на основании вероятности (табл. 2); L — величина потерь в рублях, которая определяется на основании степени тяжести нарушения (табл. 3).

Таблица 2

Преобразованные вероятности угроз к ежегодной частоте

Уровень вероятности	Описание	Частота
Незначительный	Вряд ли произойдет	0,05
Очень низкий	Событие происходит два-три раза в пять лет	0,6
Низкий	Событие происходит реже раза в год или раз в год	1,0
Средний	Событие происходит реже раза в полгода или раз в полгода	2,0
Высокий	Событие происходит реже раза в месяц или раз в месяц	12,0
Очень высокий	Событие происходит несколько раз в месяц	36,0
Экстремальный	Событие происходит несколько раз в день	365,0

Таблица 3

Последствия, преобразованные в стоимость ликвидации нарушений.

Степень тяжести нарушения	Описание	Потери, руб.
Несущественная	При осознанной угрозе нарушение не будет иметь последствий	0
Низкая	Нарушение не ведет к финансовым потерям, но выяснение характера происшествия потребует незначительных затрат	15 000
Существенная	Происшествие принесет некоторый материальный и моральный вред	150 000
Угрожающая	Потеря репутации, конфиденциальной информации. Затраты на восстановление данных, проведение расследований	1 500 000
Серьезная	Потеря клиентов, деловой репутации. Восстановление практически всех данных на электронных и бумажных носителях	3 000 000
Критическая	Потеря системы или перевод в другую безопасную среду	7 500 000

Следующим шагом обоснования инвестиций в систему информационной безопасности является проведение анализа возврата инвестиций (табл. 6). Первоначально определим затраты на внедрение системы информационной безопасности.

Для того чтобы обеспечить должный уровень безопасности, в ЗАО «Страхование» необходимо внедрить следующие элементы системы информационной безопасности: систему защиты шлюзов Интернета, систему антивирусной защиты файловых серверов и рабочих станций и систему защиты корпоративной электронной почты. Руководством в качестве поставщика решений была выбрана компания Trend Micro, которая представляет широкую линейку решений в области информационной безопасности для предприятий различного масштаба.

Затраты на внедрение комплекса решений Trend Micro приведены в табл. 5.

Период окупаемости инвестиционных проектов, связанных с внедрением информационных технологий, не должен превышать трех лет, поэтому период оценки эффективности данного проекта внедрения равен трем годам. Обозначим показатели оценки.

- $C_{ВН}$ — затраты на внедрение;
- $C_{Л}$ — затраты на покупку лицензий;
- $C_{ПР}$ — затраты на проектные работы;
- C_i — затраты на техническую поддержку;
- TCO_T — текущий показатель TCO (из отчетов «TCO Manager»);

Таблица 4

Расчет показателя ожидаемых потерь для ЗАО «Страхование»

№	Актив	Потенциальная угроза	Уровень вероятности	Степень последствия	Частота в год	Потери, руб.	ALE, руб.
1	Интернет-каналы	Разрушение ключевой инфраструктуры	Незначительный	Серьезная	0,05	3 000 000	150 000
		Отказ системы охлаждения	Средний	Существенная	2	150 000	300 000
		Нарушение конфиденциальности информации	Низкий	Серьезная	1	3 000 000	3 000 000
		Повреждение аппаратных средств инфраструктуры	Очень низкий	Угрожающая	0,6	1 500 000	900 000
		Неправильное построение инфраструктуры	Низкий	Существенная	1	150 000	150 000
		Атака на сетевую инфраструктуру провайдера	Очень низкий	Существенная	0,6	150 000	90 000
		Отказ DNS	Незначительный	Угрожающая	0,05	1 500 000	75 000
2	Система электронной почты	Атака на систему электронной почты	Очень высокий	Существенная	36	150 000	5 400 000
3	Бизнес-приложения	Проблема вывода документов на печать	Высокий	Несущественная	12	0	0
		Проблемы чтения/сохранения файлов данных	Высокий	Несущественная	12	0	0
		Нарушения надежной работы бизнес-приложений	Низкий	Угрожающая	1	1 500 000	1 500 000
		Ввод из строя корпоративной системы документооборота	Высокий	Угрожающая	12	1 500 000	18 000 000
						ИТОГО	**29 565 000**

Примечание: потенциальные угрозы, указанные в таблице TRA для ЗАО «Страхование», определены согласно рекомендациям эксперта в области информационной безопасности.

Таблица 5

Инвестиции в систему корпоративной защиты для ЗАО «Страхование»

№	Статьи затрат	Стоимость, руб.
1	Затраты на покупку лицензий	2 358 048
2	Затраты на проектные работы	369 785
3	Техническая поддержка (30 % от стоимости лицензий ежегодно)	707 414

- $TCO_Ц$ — целевой показатель TCO (из отчетов «TCO Manager»);
- $TCO_Ф$ — фактический показатель TCO;
- AS — ежегодные сбережения;
- B — выгоды при оптимизации показателя TCO;
- CF — денежный поток;
- r — ставка дисконтирования;
- $NPV_З$ — чистая приведенная стоимость затрат на проект внедрения;
- $NPV_Д$ — чистая приведенная стоимость доходов от проекта внедрения.

Затраты на внедрение системы защиты информации рассчитываются по следующей формуле:

$$C_{ВН} = C_Л + C_{ПР} + \sum_i C_i . \quad (2)$$

Выгоды от оптимизации текущего показателя TCO вычисляются по формуле:

$$B = TCO_T - TCO_Ф . \quad (3)$$

Чистые приведенные стоимости затрат на проект внедрения и доходов от проекта внедрения рассчитываются по следующим формулам:

$$NPV = \sum_{i=0}^{2} \frac{CF}{(1+r)^i} . \quad (4)$$

В первом случае роль денежного потока играют затраты на внедрение, а во втором — это выгоды от оптимизации показателя TCO и внедрения корпоративной системы защиты.

Ставка дисконтирования равна ставке рефинансирования Центрального Банка РФ.

Таблица 6

Расчет показателей возврата инвестиций на систему информационной безопасности для ЗАО «Страхование»

Показатели	Начальные затраты, руб.	1 год, руб.	2 год, руб.	3 год, руб.	Общее, руб.
Затраты на внедрение	2 358 048	369 785	707 414	707 414	4 142 661
Накопленные затраты проекта внедрения	2 358 048	2 727 833	3 435 247	4 142 661	
Ставка дисконтирования	14 %				
Чистая приведенная стоимость (NPV) затрат на проект внедрения	3 645 614				
Текущий показатель TCO	n/a	26 383 744	26 383 744	26 383 744	79 151 232
Целевой показатель TCO	n/a	19 864 933	19 864 933	19 864 933	59 594 799
Фактический показатель TCO	n/a	25 079 982	21 820 576	19 864 933	
Выгоды при оптимизации показателя TCO	0	1 303 762	4 563 167	6 518 811	12 385 740
Показатель ожидаемых потерь (ALE)	0	29 565 000	29 565 000	29 565 000	88 695 000
Эффективность системы корпоративной защиты		85 %	85 %	85 %	
Ежегодные сбережения (AS)	0	50 268	3 309 674	5 265 317	
Показатель выгод при оптимизации показателя TCO и ежегодные сбережения	0	1 354 030	7 872 841	11 784 128	21 010 999
Накопленный показатель выгод при оптимизации показателя TCO и ежегодные сбережения	0	1 354 030	9 226 871	21 010 999	
Денежный поток	–2 358 048	984 245	7 165 427	11 076 714	16 868 338
Накопленный денежный поток	–2 358 048	–1 373 803	5 791 624	16 868 338	
Чистая приведенная стоимость (NPV) доходов от проекта внедрения	10 577 426				
Внутренняя норма рентабельности (IRR)	145 %				

Внутренняя норма рентабельности рассчитывается при NPV, равном нулю.

Расчет точки безубыточности проекта внедрения корпоративной системы информационной безопасности выполнен графически (рис. 1), и точка безубыточности равна 1,6 лет.

Рис. 1. Расчет точки безубыточности проекта внедрения системы информационной безопасности

Таким образом, проект внедрения можно считать экономически выгодным, так как чистая приведенная стоимость доходов от проекта внедрения положительна и больше чистой приведенной стоимости затрат на проект внедрения в 2,9 раза.

Литература

1. *Петренко С. А., Петренко А. А.* Аудит безопасности Intranet. М.: ДМК Пресс, 2002. 416 с.
2. *Петренко С А., Симонов С. В.* Управление информационными рисками. Экономически оправданная безопасность. М.: ДМК Пресс, 2004. 400 с.
3. *Петренко С. А., Курбатов В. А.* Политики информационной безопасности. М.: ДМК Пресс, 2006. 400 с.