Анализ подходов к определению оптимального объема инвестиций в информационную безопасность

И. Б. Собакин

Аннотация. В статье приведен анализ основных подходов к определению оптимального объема инвестиций, необходимого для обеспечения информационной безопасности. Рассмотрена модель Гордона—Лоеба. Представлены исследования, опровергающие данную модель. Приведены функции нарушения информационной безопасности, функции зависимости затрат на безопасность от вероятности реализации угроз в отношении информационного актива.

Ключевые слова: *оптимальный объем инвестиций, информационная безопасность, информационный актив, оценка риска, угроза, уязвимость.*

Введение

Инвестиции в информационную безопасность позволяют не только уменьшить финансовые потери от информационных рисков, но и увеличить доходы компании, уменьшив недополученную прибыль.

Вопросы, касающиеся определения количества ресурсов, необходимых для обеспечения информационной безопасности, являются основными и требуют четкого понимания всей системы ИБ в целом. Одной из важнейших задач по обеспечению безопасности стоит выбор оптимальных технологий. Основой данного выбора является критерий правильного расчета и оценки инвестиций в безопасность. Такие инвестиции должны быть оправданы с финансовой точки зрения.

Надо сказать, что наиболее распространенной в настоящее время является именно качественная оценка рисков информационной безопасности. Основная задача такой оценки состоит в определении факторов риска, установлении потенциальных областей риска и оценке воздействия каждого их вида. Данный анализ проводится экспертным путем.

В настоящее время отмечается неточность исходных данных для расчета коэффициентов рентабельности инвестиций в информационную безопасность. Большинство организаций основываются на качественных методах оценки. Данные методы не предоставляют достаточной информации для сравнительного анализа, расстановки приоритетов и для принятия решения в целом. Таким образом, у руководства компаний появляется необходимость количественного расчета для финансового обоснования инвестиций в информационную безопасность.

1. Постановка задачи

На принятие решения об уровне инвестирования в ИБ серьезнейшим образом влияет оценка следующих трех основных факторов:

1) угрозы (вероятность возникновения угрозы; цель, квалифицированность и мотивация нарушителя; и т. п.);
2) уязвимости (степень вероятности нанесения ущерба; эффективность принимаемых мер безопасности; и т. п.);
3) затраты и выгоды (размер затрат на информационную безопасность; стоимость защищаемых активов).

Нахождение баланса между стоимостью и преимуществами системы информационной безопасности и потенциальным вредным воздействием угроз со стороны различного рода нарушителей осуществляется в условиях неопределнности и риска. Более того, результат может порой и не оправдать ожидания.

Однако субъективную составляющую данной проблемы можно минимизировать, например, следующим образом: определить области действия и границ решаемой задачи, в рамках которых возможны какие-либо измерения, и сконцентрироваться на тех аспектах, которым можно дать количественную оценку.

К ограничивающим критериям области действия и границ вышеназванной задачи можно отнести следующие.

1. Коммерческая направленность организаций и связанные с ней стратегические цели бизнеса. (Процедура определения потенциальных потерь

вследствие нарушения безопасности информационных активов, представляющих особую важность для общества или государства, чрезвычайна сложна и зачастую невозможна.)

2. Отсутсвие рассмотрения ситуации конфликта интересов между специалистом в области информационной безопасности и руководством и ее влияния на оптимальный уровень инвестиций в ИБ.
3. Исключение ситуаций, когда некоторые инвестиции в ИБ обеспечивают защиту сразу нескольких информационных активов, имеющих схожие риски. (Так, противопожарная безопасность обеспечивает защиту как информационных, так и неинформационных активов.)
4. Ожидаемые потери, связанные с нарушением целостности, доступности и конфиденциальности рассматривать как выражение стоимости информационных активов, исследуемых в качестве объекта риска.

Несмотря на отсутствие простой процедуры определения вероятностей возникновения и реализации угроз в отношении информационного актива, представляется целесообразным сконцентрироваться именно на количественных аспектах. И с учетом проработанности исследований анализ информационных рисков начинать с решения задачи определения оптимального размера инвестиций, необходимого для обеспечения информационной безопасности предприятия.

2. Анализ основных подходов

Разработки в области нахождения экономически обоснованного объема денежных средств, необходимого для обеспечения ИБ, нашли свое отражение как зарубежных, так и в отечественных работах. Однако именно зарубежные работы последнего десятилетия являются передовыми и на их основе целесообразнее всего провести дальнейший анализ.

Экономическая модель Гордона—Лоеба [6] позволяет найти оптимальный размер инвестиций в ИБ и при проведении исследований является в настоящее время основополагающей.

Модель Гордона—Лоеба представляет собой довольно обобщенную модель оценки уменьшения уязвимости системы как результат увеличения инвестиций в информационную безопасность. Авторы рассматривают два определенных класса функций, которые отражают возможный сценарий уменьшения уязвимости системы и приходят к заключению, что для каждого класса оптимальный уровень инвестиций не превышает $\frac{1}{e} \approx 36{,}8\ \%$ от ожидаемых потерь вследствие нарушения ИБ. Вопрос об универсальности применения данных расчетов авторы оставили открытым.

Для оценки оптимального уровня инвестиций в информационную безопасность с целью защиты некоторого информационного актива авторы [6] предлагают следующие обозначения:

λ — потери от осуществления угрозы;

t — вероятность возникновения угрозы;

ν — вероятность реализации угрозы.

Авторы ограничивают вероятности возникновения и реализации угрозы, следующим образом:

$$0 < t < 1 \quad \text{и} \quad 0 < \nu < 1 .$$

Так как вероятность возникновения угрозы взята авторами за константу, для простоты использования введено обозначение $L = t \times \lambda$, где L означает потери или потенциальные потери, связанные с информационным активом.

Введен параметр $z > 0$, означающий затраты на обеспечение защиты информационного актива (в денежном выражении). Так, z измеряется в тех же единицах, что и потенциальные потери L. Цель затрат на обеспечение защиты z состоит в уменьшении вероятности того, что информационному активу будет нанесен ущерб.

Функция $S(z,\nu)$ представляет собой вероятность реализации угрозы с применением защиты актива — инвестиций в ИБ. Авторы рассматривают функцию $S(z,\nu)$ как дважды непрерывно дифференцируемую со следующими условиями.

A1. $\forall z \in R$, $S(z,0) = 0$. Если информационный актив полностью неуязвимый, то он будет оставаться идеально защищенным независимо от объема вкладываемых инвестиций, даже и при их отсутствии вовсе.

A2. $\forall \nu \in (0,1)$, $S(0,\nu) = \nu$. При отсутствии инвестиций в информационную безопасность вероятность реализации угрозы останется неизменной.

A3.

$$\forall \nu \in (0,1),\ \forall z \in R,\ \frac{\partial}{\partial z} S(z,\nu) < 0$$

$$\text{и}\ \frac{\partial^2}{\partial z^2} S(z,\nu) > 0 .$$

Если объем инвестиций в информационную безопасность увеличивается, информация становится более защищенной, причем

$$\forall \nu \in (0,1),\ \lim_{z \to \infty} S(z,\upsilon) = 0 .$$

Таким образом, инвестируя значительные суммы в обеспечение информационной безопасности, вероятность реализации угрозы может приблизиться к нулю.

Ожидаемая прибыль от вложения инвестиций в информационную безопасность (Expected Benefits of

an Investment in Information Security, *EBIS*) рассматривается как уменьшение ожидаемых потерь организации вследствие увеличения инвестиций в ИБ:

$$EBIS(z) = [\nu - S(z,\nu)]L . \quad (1)$$

Ожидаемая чистая прибыль от вложения инвестиций в ИБ (Expected Net Benefits from an Investment in Information Security, *ENBIS*) равна разности *EBIS* и стоимости инвестиций:

$$ENBIS(z) = [\nu - S(z,\nu)]L - z . \quad (2)$$

Для того чтобы сфокусироваться на уменьшении вероятности реализации угрозы, авторы обозначают оптимальный размер инвестиций как $z^*(\nu)$.

Далее авторы приводят два класса функций вероятности нарушения безопасности, удовлетворяющих условиям **A1–A3**.

Первый класс функций:

$$S^I(z,\nu) = \frac{\nu}{(\alpha z + 1)^\beta}, (\alpha > 0, \beta \geq 1) . \quad (3)$$

Второй класс функций:

$$S^{II}(z,\nu) = \nu^{\alpha z + 1}, (\alpha > 0) . \quad (4)$$

Анализ первого класса функций вероятности нарушения безопасности показал, что функция оптимальных инвестиций (z^*) постоянно возрастает с увеличением вероятности реализации угроз (ν) (рис. 1). Что касается второго класса функций, то функция z^* сначала возрастает, а затем уменьшается с увеличением ν (рис. 2).

Далее авторы приводят предположение и показывают, что для двух классов функций вероятности нарушения информационной безопасности оптимальные инвестиции в ИБ всегда меньше или равны 36,79 % от ожидаемых потерь в отсутствие каких-либо инвестиций.

Допущение того, что функция предельной прибыли от увеличения вложений в информационную безопасность будет убывать, исходит как из интуитивных соображений, так и из предварительных и последовательных эмпирических обоснований, данных в работе [4]. Авторы дали оценку модели Гордона—Лоеба и экспериментально подтвердили представленные ими предположения. Эмпирическим путем было доказано, что нарушение информационной безопасности, связанное с распространением компьютерных вирусов по электронной почте, наиболее точно описывается классом функций $S^{II}(z,\nu)$, нежели $S^I(z,\nu)$.

Немного позже модель Гордона—Лоеба была расширена по нескольким направлениям. Среди первых исследований, опровергающих и проверяющих на прочность данную модель, является работа автора [5]. В данной работе проводится анализ несколько иных и различных по себе классов функций нарушения информационной безопасности (рис. 3). Автор Kjell Hausken считает, что существуют и другие условия для более актуального построения функции прибыли от вложений в информационную безопасность.

Автор полагает, что логистическая функция[1], которая сначала возрастает, а потом убывает, может быть более полезна для объяснения прибыли от вложений в ИБ. Приводится следующая функция:

$$S^{III}(z,\nu) = \frac{\nu}{1 + \gamma(e^{\varphi z} - 1)}, (\varphi > 0, \gamma > 0). \quad (5)$$

Данная функция удовлетворяет условиям A1 и A2 модели Гордона—Лоеба и новому условию A4:

A4. $\forall \nu \in (0,1)$ и $\forall z \in R$, $\frac{\partial}{\partial z} S(z,\nu) < 0$;

$$\frac{\partial^2}{\partial z^2} S(z,\nu) < 0 \text{ при } 0 \leq z < z_i, \frac{\partial^2}{\partial z^2} S(z,\nu) > 0$$

при $z > z_i$, где z_i — некоторый промежуточный размер инвестиций, причем:

$$\frac{\partial^2}{\partial z^2} S(z_i,\nu) = 0 \text{ и } \lim_{z\to\infty} S(z,\upsilon) = 0 \text{ для всех } z .$$

В следующем разделе автор приводит уже другую функцию:

$$S^{IV}(z,\nu) = \begin{cases} \nu(1 - \mu z^k), z \leq \mu^{-1/k} = z_u, \\ 0, z > \mu^{-1/k}, 0 < k < 1, \end{cases} \text{ где } \mu > 0. \quad (6)$$

Данная функция удовлетворяет условиям A1 и A2 модели Гордона—Лоеба и уже новому условию A5:

A5.

$$\forall \nu \in (0,1) \text{ и } z \leq z_u > 0, \frac{\partial}{\partial z} S(z,\nu) < 0, \frac{\partial^2}{\partial z^2} S(z,\nu) > 0,$$

$S(z,\nu) = 0$ для всех $z > z_u$.

Функция $S^{IV}(z,\nu)$ привносит качественно новый результат. Функция $\nu(1 - \mu z^k)$ проходит через ось

[1] Логистическая функция — функция от одного аргумента, график которой сначала растет медленно, потом быстро, а затем снова замедляет свой рост, стремясь к какому-то пределу. Она моделирует кривую роста вероятности некоего события, по мере изменения управляющих параметров (факторов риска). Часто применяются в анализе спроса на товары, обладающие способностью достигать некоторого уровня насыщения, и для объяснения различных явлений (рост населения, распространение вирусов, финансовые кризисы и т. д.).

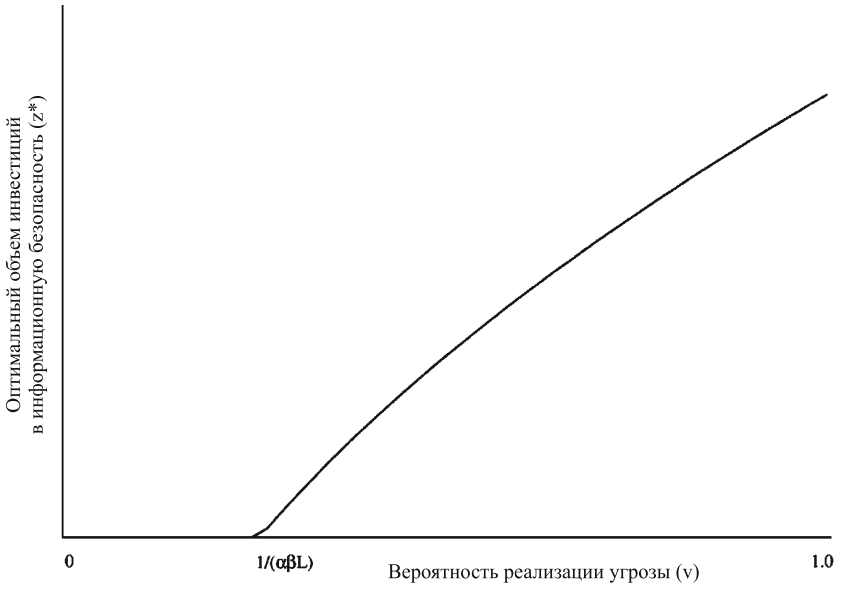

Рис. 1. Оптимальный уровень инвестиций для первого класса функций

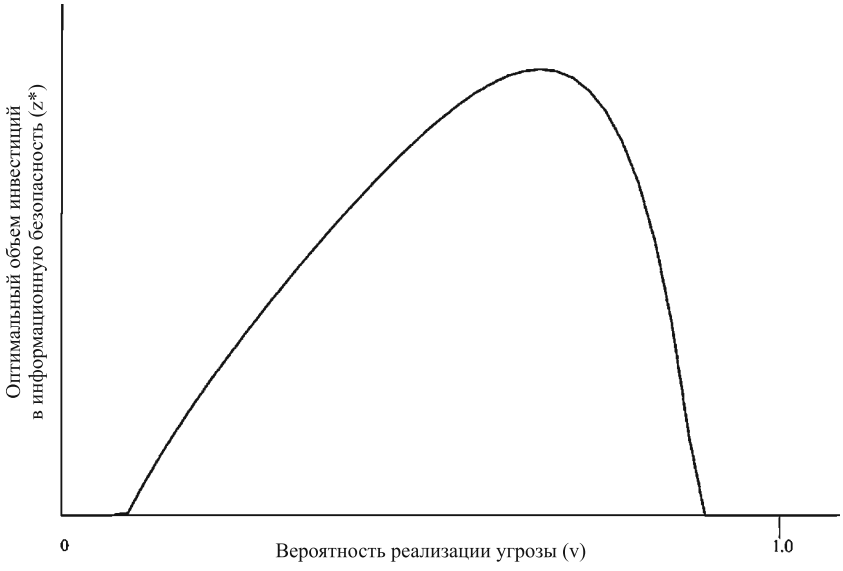

Рис. 2. Оптимальный уровень инвестиций для второго класса функций

абсцисс при $z = \mu^{-1/k}$. Таким образом, это значит, что вероятность нарушения безопасности можно свести к нулю.

В качестве очередного пятого класса функций нарушения безопасности автор приводит:

$$S^V(z,\nu) = \begin{cases} \nu(1-\omega z^k), z \le \omega^{-1/k} = z_u, \\ 0, z > \omega^{-1/k}, k > 1, \end{cases} \text{ где } \omega > 0. \qquad (7)$$

Функция удовлетворяет условиям A1, A2 и условию A6:

A6.

$\forall \nu \in (0,1)$ и $z \le z_u > 0$, $\frac{\partial}{\partial z} S(z,\nu) < 0$, $\frac{\partial^2}{\partial z^2} S(z,\nu) < 0$, $S(z,\nu) = 0$ для всех $z \ge z_u$.

Рассматривая поведение функции $S^V(z,\nu)$, удовлетворяющей условию A6, автор уточняет, что с постепенным увеличением инвестиций в ИБ увеличивается и положительный эффект. В итоге вероятность нарушения безопасности достигает нулевого значения.

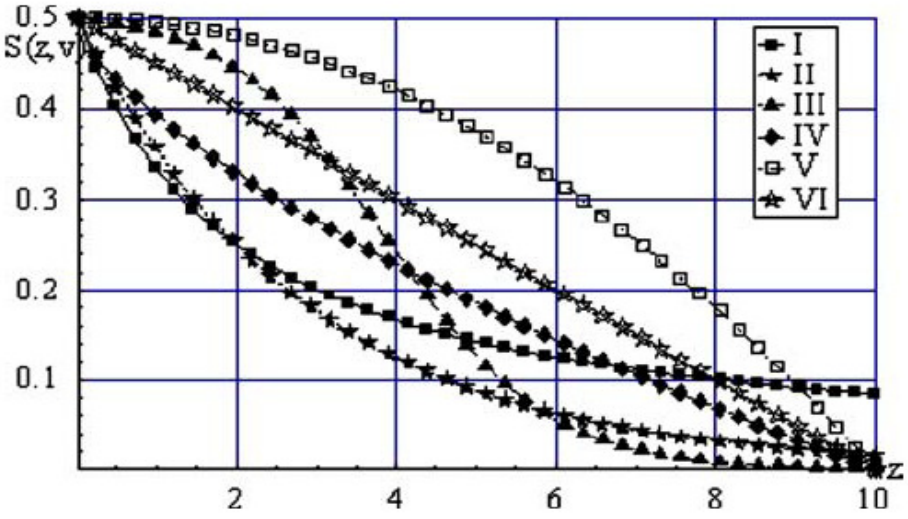

Рис. 3. Функции нарушения информационной безопасности

И, наконец, автор представляет шестой класс функций:

$$S^{VI}(z,\nu)=\begin{cases}\nu(1-\lambda z), z\le 1/\lambda = z_u,\\ 0, z>1/\lambda,\end{cases} \text{ где } \lambda>0. \qquad (8)$$

Функция удовлетворяет условиям A1, A2 и условию A7:

A7.

$$\forall \nu\in(0,1) \text{ и } z\le z_u>0,\ \frac{\partial}{\partial z}S(z,\nu)<0,\ \frac{\partial^2}{\partial z^2}S(z,\nu)=0,$$

$S(z,\nu)=0$ для всех $z\ge z_u$.

В представленном случае функция $S^{VI}(z,\nu)$ является линейной.

Таким образом, автор рассмотрел 4 вида классов функций предельной прибыли от вложений в информационную безопасность. В своем исследовании автор представил такие классы, где оптимальный уровень инвестиций в ИБ превышает порог в $1/e$ от ожидаемых потерь, вступая, таким образом, в противоречие с моделью Гордона—Лоеба.

В этом же году автор Jan Willemson в своей работе [1], оспаривая и немного изменяя условие **A3** модели Гордона—Лоеба, указывает на то, что оптимальный уровень инвестиций в информационную безопасность может превысить известный порог в 36,8 % от ожидаемых потерь вследствие нарушения ИБ.

Автор констатирует, что в реальном мире существуют такие ситуации, в которых потенциальная угроза может быть полностью устранена (так, например, существует возможность избавится от представляющего угрозу человека навсегда).

Автор предлагает изменить условие непрерывности второй производной функции нарушения ИБ:

A3'.

$$\frac{\partial}{\partial z}S(z,\nu)\le 0 \text{ и } \frac{\partial^2}{\partial z^2}S(z,\nu)\ge 0.$$

Таким образом, учитывая условие существования вероятности реализации угрозы равной нулю, он доказывает, что оптимальный уровень инвестиций в информационную безопасность может достигать вплоть до 100 % от ожидаемых потерь вследствие нарушения ИБ.

Позже Willemson усовершенствовал модель Гордона—Лоеба по двум направлениям [2], в первую очередь, добавив условие **A4:** $\frac{\partial}{\partial z}S(z,\nu)>0$, а также обобщив все предложенные за последнее время модели в унифицированную форму:

$$S^{\Diamond}(z,\nu)=\nu^{p(z)}q(z). \qquad (9)$$

Так, $S^{I}(z,\nu)=\frac{\nu}{(\alpha z+1)^{\beta}}$ удовлетворяет $S^{\Diamond}(z,\nu)$ при $p(z)=1,\ q(z)=\frac{1}{(\alpha z+1)^{\beta}}$, $S^{II}(z,\nu)=\nu^{\alpha z+1}$ удовлетворяет $S^{\Diamond}(z,\nu)$ при $p(z)=\alpha z+1,\ q(z)=1,$ и т. д.

В работе [3] K. Julisch дает ответы на следующие вопросы: как минимизировать потери от угроз информационной безопасности, как распределить бюджет между несколькими информационными

системами (направлениями защиты информации) и сколько вообще тратить на безопасность. Касательно оптимального бюджета информационной безопасности, то он определяется по формуле:

$$B_{opt} = \sqrt{EL_{actual} \times B_{actual}}, \quad (10)$$

где B_{actual} — текущий бюджет средств, выделяемых на ИБ, EL_{actual} — ожидаемые потери, полученные эмпирическим путем.

Таким образом, автор смещает акцент с нахождения оптимального размера на ИБ на определение того, «стоит ли повышать бюджет ИБ на очередной дополнительный доллар».

Заключение

Авторами были проведены серьезные исследования, которые позволили усомниться в истинности результатов и заключений, сделанных в работе Гордона—Лоеба. Однако актуальность необходимости математического обоснования размера оптимальных инвестиций в ИБ данные работы не исключают, более того — обращают внимание на сложность рассматриваемых процессов.

Представляется, что дальнейшее усложнение данной модели с математической точки зрения, не опираясь на конкретные статистические данные, не представляет ценности для последующего практического применения.

Таким образом, одним из основных направлений совершенствования модели является проведение эмпирических исследований, при этом необходимо обращать внимание на то, как организации инвестируют в информационную безопасность, как они оценивают потенциальные потери, вероятности возникновения и реализации угроз на практике.

Литература

1. *Willemson J.* On the Gordon & Loeb Model for Information Security Investment. In Proceedings of The Fifth Workshop on the Economics of Information Security (WEIS 2006), 2006.
2. *Willemson J.* Extending the Gordon&Loeb Model for Information Security Investment. Fifth International Conference on Availability, Reliability, and Security (ARES 2010), 2010.
3. *Julisch K. A.* Unifying Theory of Security Metrics with Applications. Research Report, 2009.
4. *Tanaka H., Matsuura K.* Vulnerability and Effects of Information Security Investment: A Firm Level Empirical Analysis of Japan // In International Forum of Financial Information Systems and Cybersecurity: A Public Policy Perspective, College Park, MD, May 26, 2005.
5. *Hausken K.* Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability. Information Systems Frontiers, 5(8), 2006.
6. *Lawrence A. Gordon, Martin P. Loeb.* The Economics of Information Security Investment. ACM Transactions on Information and System Security, 5:438–457, November 2002. Reprinted in Economics of Information Security, 2004, Springer, Camp and Lewis, eds.

Собакин Иван Борисович. Аспирант Московского государственного индустриального университета. Окончил МГИУ в 2008 г. Количество печатных работ: 3. Область научных интересов: оценки информационных рисков. E-mail: sobakin86@mail.ru