К. С. Барабанов

РАСЧЕТ ОПТИМАЛЬНЫХ ИНВЕСТИЦИЙ В ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ

В силу отсутствия законодательных и нормативных актов (государственного и международного уровней), направленных против хищения результирующих информационных ресурсов и продуктов, которые не защищены патентами, но являются объектами индустриальной собственности (альтернативные решения, поисковые концепции и т. п.), существует значительное поле деятельности в домене информационной индустрии, которое связано с поиском эффективных и дееспособных решений по созданию моделей обеспечения конфиденциальности в корпоративных информационных системах.

Современные компании зачастую используют очень сложные средства экономического анализа учета внутренних ресурсов с целью повышения доходности и сокращения издержек и возможных потерь. Однако только малая доля этих компаний пытается применить методики подобного анализа в случае оценки инвестиций в технологии обеспечения конфиденциальности информационных ресурсов. Отсутствие оптимальных оценочных методик заставляет организации, использующие средства количественного анализа, вкладывать значительные ресурсы в поддержание систем обработки внутренней информации.

Применение инструментов эконометрики для оценки обеспечения конфиденциальности корпоративных информационных ресурсов (КИР) обусловлено большими потенциальными возможностями методов экономического анализа, базирующихся, в частности, на статистических моделях воздействий и методах численного оценивания системных реакций, возможностями математического анализа и синтеза простых и сложных систем различного функционального назначения. Сдерживающим фактором при этом является отсутствие на практике необходимых исходных данных, в частности статистики угроз нарушения конфиденциальности для конкретного объекта защиты, общепринятой шкалы значимости (ценности) информации, нормативных категорий уровней защиты и пр.

За последние несколько лет было проведено большое количество исследований по экономическим аспектам безопасности информационных систем. Труды, отражающие результаты данных исследований, было бы удобно разделить на несколько групп. К первой группе относится литература, описывающая оценки экономической выгоды от инвестиций в информационную безопасность. В работе [1] описана система экономического моделирования для оценки оптимальных инвестиций в информационную безопасность для защиты заданного количества информации. Во

второй группе акцент делается на индивидуальные технологии обеспечения безопасности. Так, в [2] исследуется оценка системы обнаружения вторжений в общей архитектуре информационной безопасности компании. Третья группа — это набор руководств для принятия решений об уровне инвестиций в информационную безопасность. В [3] представлена аналитическая модель, способствующая принятию решения о величине инвестиций в информационную безопасность. В [4] показано, как начальник службы информационной безопасности может практически использовать метод Саати — Analityc hierarchy process (процесс иерархической аналитики) [5] для наиболее рационального расходования средств ИТ-бюджета на информационную безопасность.

Наиболее практически применимыми для оценки обеспечения конфиденциальности КИР представляются рекомендации литературы третьей группы. Однако описываемые аналитические модели предполагают проведение достаточно сложных и субъективных промежуточных оценок. Так, к примеру, рассматривая процесс иерархической аналитики, нельзя не отметить, что при очевидном удобстве данного метода (возможность детализации ценностей и последующей свертки всех конкретных оценок в интегральный показатель) серьезные исследования последнего десятилетия приводят к выводу, что корректнее и надежнее использовать парные сравнения для получения только качественных заключений [6].

Авторы [1] представили простую и обобщенную модель оценки сокращения угроз конфиденциальности КИР как результат увеличения инвестиций в информационную безопасность. Они рассмотрели два определенных класса функций, которые отражают возможный прогноз уменьшения количества уязвимостей, и пришли к выводу, что для каждого из них оптимальный уровень инвестиций не превышает $\frac{1}{e} \approx 36{,}8\%$ от общей стоимостной оценки защищаемой информации. При этом вопрос об универсальности данной константной величины для всех функций, удовлетворяющих заданным ограничениям, авторы оставили открытым. В [7] автор приводит доказательство существования функций (удовлетворяющих заданным ограничениям) уменьшения уязвимостей, требующих инвестиций на уровне 50 % от оценочной стоимости информации, что делает выводы авторов [1] неверными. Также рассматривается ряд прогнозов, при которых уровень инвестиций составил бы 100 %, если опустить требование непрерывности второй производной функции уменьшения уязвимостей.

В литературе часто встречаются описания методик оценки и управления расходами на информационную безопасность, опирающихся на понятие ежегодных ожидаемых потерь ALE (annual loss expected). При этом

$$ALE = R \cdot V,$$

где R — ожидаемый размер потерь при реализации угрозы нарушения конфиденциальности КИР;

V — оценочная стоимость потерь.

В отличие от моделей, базирующихся на подобных критериях оценки, более удачной стоит признать модель, где за основу взято понятие среднего экономического риска. Экономические критерии, базирующиеся на сопоставлении ущерба от угроз и затрат на безопасность, определяют уровни рациональных общих и частных ассигнований на безопасность [8, 9]. Применим данный подход к оценке инвестиций в обеспечение конфиденциальности корпоративных информационных ресурсов.

Формально любую систему обеспечения конфиденциальности КИР можно рассматривать как некоторое решающее устройство, на вход которого поступают в форме физических воздействий информационные угрозы. Решающее устройство, действуя в определенном пространстве ограничительных условий (законодательных, ресурсно-видовых, стоимостных и др.), реагирует на входные воздействия с помощью кадровых и материально-технических ресурсов. Реакция представляет собой реализацию нескольких взаимосвязанных функций, в число которых входят:

· выявление, в том числе опережающее, угроз;

· блокирование угроз;

· нейтрализация угроз;

· ликвидация последствий реализаций угроз и др.

Основой подхода к изучению показателей, характеризующих систему информационной защиты и оптимизированных функциональных критериев, стало понятие среднего экономического риска и связанные с ним понятия эффективности и рентабельности защиты.

Под эффективностью защиты КИР понимается величина

$$E = \frac{\sum_{i=1}^{N} p_i C_i \psi_i}{\sum_{i=1}^{N} p_i C_i},$$

где N — число угроз нарушения конфиденциальности КИР;

ψ — булевская функция, принимающая значение 1, если защита от угрозы с номером k предусмотрена, и 0 — в противном случае;

ρ — вероятность угрозы с заданным номером;

C — значимость угрозы.

Показатель E находится в прямой зависимости от уровня инвестиций в информационную безопасность B. Зависимость монотонно растущая. В пределе, при очень больших затратах B, величина E стремится к 1.

Конкретный вид зависимости $E=E(B)$ определяется многими факторами: видом используемых ресурсов, распределением их по пространству угроз, видами используемых средств защиты, способами организации противодействий и др. Наилучшим (оптимальным) вариантом зависимости будет та, при которой для каждого уровня ассигнований B будет иметь место максимальное значение величины E. Этот вариант определяет один из критериев стратегии информационной защиты.

Особый интерес представляет случай, когда ассигнования B на безопасность велики. При оптимальном расходовании этих средств эффективность защиты должна быть близкой к 100 %, асимптотически приближаясь к этому пределу по мере увеличения величины B.

Исследования сферы высоконадежных решений в домене безопасности информационных ресурсов при оптимальных затратах на безопасность выявляют однозначную связь между инвестициями B и величиной E. Для этого рассматривается функция E в области значений, близких к 100 %.

Важно подчеркнуть, что стремление к максимальной эффективности защиты E путем роста затрат B на безопасность может привести к новой опасности — возможности разориться из-за слишком больших расходов на защиту. Средства на инвестиции в информационную безопасность берутся из прибыли, уменьшая тем самым ее долю, отводимую для решения основных производственных задач.

Разумную границу ассигнований можно оценивать путем сопоставления экономии средств при защите КИР и затрат на безопасность. Для этого введем показатель общей рентабельности защиты КИР ρ:

$$\rho = E - \frac{B}{R_0},$$

где R_0 — абсолютная стоимость прогнозируемого информационного ущерба (начальный риск).

Критерием оптимальности системы информационной защиты является условие максимума рентабельности защиты. Ищется этот максимум путем вариации суммарных инвестиций в информационную безопасность B и распределения их по пространству угроз. Добавляя к этому критерию обеспечение максимума эффективности защиты E при заданном уровне ассигнований B, получаем следующий обобщенный критерий: система обеспечения конфиденциальности КИР должна обеспечивать наибольшую рентабельность при максимальной эффективности защиты:

$$\max_{(B)} \rho \quad \max_{(d)} E(*),$$

где d — пространство средств и способов защиты.

Данная аналитическая модель не может претендовать на полноту описания домена оптимальных инвестиций в информационные системы обеспечения конфиденциальности КИР, однако является вспомогательной для дальнейшего исследования зависимостей вида $E(B)$, а точнее, асимптотических приближений функции в областях, близких к 100 %. Также обобщенный критерий (*) может быть использован для поддержки принятия решений по экспертным оценкам параметризированных компонентов информационных систем обеспечения конфиденциальности корпоративных информационных ресурсов.

СПИСОК ЛИТЕРАТУРЫ:

1. *Gordon L. A., Loeb M. P.* The economics of information security investment // ACM Transactions on Information and Systems Security. 2002. Vol. 5. № 4. P. 438–457.
2. *Cavusoglu H., Mishra B., Raghunathan S.* The value of intrusion detection systems in information technology security architecture // Information Systems Research. 2005. Vol. 16. № 1. P. 28–46.
3. *Cavusoglu H., Mishra B., Raghunathan S.* A model for evaluating IT security investments // Communications of the ACM. 2004. Vol. 47. № 7. P. 87–92.
4. *Bodin L. D., Gordon L. A., Loeb M. P.* Evaluating information security investments using the analytic hierarchy process // Communications of the ACM. 2005. Vol. 48. № 2. P. 79–83.
5. *Саати Т.* Принятие решений. Метод анализа иерархий. М.: Радио и Связь, 1993.
6. *Горский П.* Введение в дисциплину «Поддержка принятия решений». URL: http://www.gorskiy.ru/articles.html.
7. *Willemson J.* On the Gordon & Loeb Model for Information Security Investment // The Fifth Workshop on the Economics of Information Security (WEIS 2006). 2006.
8. *Soo Hoo K. J.* How much is enough? A risk-management approach to computer security. PhD thesis. Stanford University, 2001. URL: http://iis-db.stanford.edu/pubs/11900/soohoo.pdf.
9. *Дубров А. М., Лагоша Б. А., Хрусталев Е. Ю.* Моделирование рисковых ситуаций в экономике и бизнесе. М.: Финансы и статистика, 1999.