ББК У9(2), 0

ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

© 2004 В. Ю. Карпычев

ГУ НПО «Специальная техника и связь»

Рассматриваются вопросы инвестиционного анализа разрабатываемых систем информационной безопасности. Дается классификация категорий ущерба и оцениваются риски и уровни нарушения информационной безопасности.

Описывается порядок выбора допускаемого уровня риска.

В условиях рыночной экономики любой хозяйствующий субъект (ХС) при ограниченности финансовых ресурсов имеет широкий спектр инвестиционных возможностей. Поэтому для оптимизации инвестиционного портфеля необходимо правильно оценивать эффективность инвестиционных проектов. Это положение полностью относится к информационным технологиям (IT), которые менеджеры рассматривают как средство решения задач бизнеса: снижение издержек производства, повышение производительности критичных для бизнеса операций и т. д.

Однако в этом подходе существует исключение: цели инвестиций в системы информационной безопасности (СИБ) отличаются от стандартных целей IT-инвестиций. В контексте СИБ нельзя говорить о непосредственном возврате инвестиций, так как они не предполагают потока будущих денежных поступлений, покрывающих инвестиции.

С экономической точки зрения инвестиции в СИБ

1. Имеют целью предотвращение (снижение) ущерба от возможного нарушения ИБ, а не получение дополнительных экономических выгод.

2. Сами являются для ХС специфическим экономическим ущербом.

3. Экономически целесообразны, если их размер не превышает размера возможного ущерба.

Эти идеи определяют основные направления инвестиционного анализа СИБ: оценку ущерба в случае реализации угроз ИБ и оценку затрат на создание СИБ.

Анализ ущерба при реализации угроз информационной безопасности. Очевидно, что любой объект ИБ обладает некоторой *ценностью*. Однако количественная оценка ценности информации имеет особенности и связана с большими трудностями. Поэтому наиболее характерна качественная оценка ценности объекта ИБ, например, малоценный, средней ценности, ценный и т. д.

При реализации *угрозы* в отношении конкретного объекта ИБ можно говорить об *ущербе* объекту, который определяется в процентах от ценности объекта.

Категории ущерба. Традиционно под ущербом понимаются материальные потери, оцениваемые в количественном или стоимостном исчислении. При этом игнорируются иные отрицательные результаты реализации угроз. Поэтому более корректно выделение не только «материального», но и «нематериального» ущерба.

Под *материальным ущербом* понимается ущерб, который характеризуется количественно измеримыми показателями и имеет непосредственную и, возможно, функциональную связь с финансовыми показателями ХС.

Нематериальным ущербом можно считать ущерб, нанесенный *гудвилу* ХС: имиджу, репутации, конкурентным преимуществам и пр. В современной экономике нематериальный ущерб оказывает значительное влияние на экономическую безопасность ХС. Так, «снижение уровня конкурентоспособности» предполагает потери в продвижении продукции, которое, в свою очередь, связано с другими показателями, например таким, как

«неудовлетворенность клиентов».

Расчет нематериального ущерба очень сложен, поскольку нематериальные потери оцениваются субъективными показателями с лингвистическими или «балльными» значениями.

Вероятность нанесения ущерба. Кроме абсолютной величины существенную роль при экономическом анализе имеет вероятность нанесения ущерба. В данном контексте под *вероятностью* понимается мера уверенности в том, что какое-либо событие произойдет в действительности. Она также оценивается лингвистически или в баллах. Для оценки вероятности ущерба можно использовать *частоту реализации угрозы* за определенный период времени.

Риск нарушения информационной безопасности. Как известно, деятельность ХС, которая сопровождается вероятным появлением ущерба, считается *рисковой*. Для качественной оценки риска обычно используются табличные методы. В простейшем случае используется субъективная оценка двух факторов: *вероятности угрозы* и *величины ущерба*. Двухфакторная оценка моделирует ситуацию отсутствия на предприятии СИБ. В этом случае реализованная угроза ведет к нанесению ущерба объекту ИБ.

При наличии СИБ модель риска должна учитывать способность системы противодействовать реализации угрозы. Для этого модель может быть дополнена фактором *уязвимости* СИБ, а риск должен учитывать вероятность преодоления СИБ при реализации угрозы. Поэтому вероятность нанесения ущерба уже не равна вероятности реализации угрозы.

Ранжирование рисков. Для формирования решений по противодействию угрозам целесообразно оценить степень опасности каждой угрозы и, используя эти данные, произвести их ранжирование. Эту задачу удобно решать на основе таблицы рисков, которая представляет собой матрицу угроз и поставленных им в соответствие рисков.

Множество количественно оцененных рисков позволяет построить стек угроз (последовательность убывающих значений рисков). Таблица и стек рисков могут быть использованы для анализа с целью выявления угроз (уязвимостей) в стеке, которые обеспечивают наибольший вклад в значение интегрального риска.

После процедуры спецификации и оценки риска аудит ИБ может быть ограничен теми рисками, которые реальны для этого предприятия.

Выбор допустимого уровня риска. Выбор допустимого уровня риска связан с затратами на реализацию СИБ. В простейшем случае могут быть реализованы так называемый базовый уровень или повышенный уровень ИБ.

Базовый уровень ИБ обязателен для любой IT. Для его обеспечения используется упрощенный подход к анализу рисков, при котором рассматривается стандартный набор наиболее распространенных угроз безопасности (вирусы, сбои оборудования, несанкционированный доступ и т. д.).

Для противодействия этим угрозам принимается типовой набор решений по обеспечению ИБ вне зависимости от вероятности их осуществления и уязвимости ресурсов. Поэтому характеристики угроз на базовом уровне и вопросы эффективности обеспечения ИБ не рассматриваются. Подобный подход приемлем, если ценность объектов ИБ не является чрезмерно высокой.

Затраты на аппаратно-программные средства ИБ и организационные мероприятия, необходимые для соответствия информационной системы базовым спецификациям, являются обязательными. Дополнительные затраты, обоснованные результатами аудита ИБ, не должны превышать 5-15 % средств, необходимых для работы информационной системы.

Второй подход применяется при обеспечении *повышенного уровня* безопасности. Для этого проводится анализ рисков в полном объеме: определяется ценность ресурсов; к стандартному набору добавляется список угроз, актуальных для конкретной информационной системы; оцениваются вероятности угроз; определяются уязвимости ресурсов.

Обычно проводится анализ по критерию «стоимость/эффективность» нескольких вариантов защиты. В зависимости от степе-

ни готовности ХС к совершенствованию ИБ и характера основной деятельности обоснование выбора допустимого уровня риска может проводиться разными способами.

При этом следует иметь в виду, что ущерб от нарушения ИБ может быть значительно ниже стоимости СИБ (т. е. речь идет об избыточно надежной СИБ). И, следовательно, основной ущерб ХС связан не с потерями от нарушения ИБ, а с чрезмерно высокой стоимостью системы. Поэтому инвестиции в создание и эксплуатацию СИБ должны быть сбалансированы и соответствовать масштабу угроз.

Такой качественный анализ показывает, что в инвестиционном диапазоне существует оптимальное значение инвестиций в СИБ, минимизирующее *общий ущерб* при нарушениях ИБ. Именно в этом смысле рассматривается задача создания экономически оптимальной СИБ для ХС.

Применение даже недорогих способов и средств обеспечения ИБ резко снижает суммарный ущерб. Поэтому инвестиции в СИБ в сравнительно небольших размерах очень эффективны.

Рост затрат на СИБ сверх оптимального значения ведет к увеличению ущерба. В этом случае повышение надежности СИБ и соответствующее снижение вероятности ущерба нивелируется чрезмерно высокой стоимостью самой СИБ. Поэтому наилучшей стратегией, видимо, является использование СИБ, обеспечивающей минимум ущерба.

В случае, когда доминирующим требованием является обеспечение гарантированной ИБ на заданном уровне, реализация концепции экономически оптимальной СИБ не применима. Это относится, например, к конфиденциальным сведениям государственных организаций.

ECONOMIC ASPECTS OF ENSURING INFORMATION SECURITY

© 2004 V. Yu. Karpychev

Privolzhsky Branch of State Institution “Research and Production Association “Specialized Equipment and Communication” of the Ministry of Home Affairs of Russia

Issues of investment analysis of information system security are discussed. Classification of damage categories is given. Risks and levels of affecting information security are assessed.

The order of choosing the acceptable risk level is described.