УДК 33:004.056

ПОДХОДЫ И МЕТОДЫ ОБОСНОВАНИЯ ЦЕЛЕСООБРАЗНОСТИ ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Нурдинов Р. А., Батова Т. Н.

Национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, Россия (197101, Санкт-Петербург, пр. Кронверкский, д.49), e-mail: org@mail.ifmo.ru

Для решения проблемы выбора средств защиты информации (СЗИ) предлагается использовать два подхода: первый основан на оценке конкурентоспособности, второй – на оценке целесообразности их использования для конкретного объекта защиты. Проведён обзор методов оценки конкурентоспособности СЗИ, среди которых наиболее подходящими являются: метод, основанный на нахождении интегрального показателя конкурентоспособности, метод экспертных оценок и метод тестирования. Разработано два метода оценки целесообразности использования СЗИ для конкретного объекта защиты: метод определения коэффициента нейтрализации угроз и метод анализа рисков информационной безопасности. Метод нахождения коэффициента нейтрализации угроз основан на экспертных оценках и носит субъективный характер. Метод, основанный на анализе рисков, предполагает определение экономической выгоды от использования СЗИ. Кроме того, на основании значения затратоёмкости информационных активов принимается решение о выборе оптимального набора средств защиты информации для конкретного объекта защиты.

Ключевые слова: информационный актив, средства защиты информации (СЗИ), риск информационной безопасности, объект защиты, модель угроз, коэффициент нейтрализации угроз, коэффициент экономической эффективности, рискоёмкость, затратоёмкость обеспечения безопасности.

APPROACHES AND METHODS OF RATIONALE CHOOSING OF INFORMATION PROTECTION FACILITIES

Nurdinov R. A., Batova T. N.

Research university of information technologies, mechanics and optics, St. Petersburg, Russia (197101, Saint Petersburg, Kronverkskiy pr., 49), e-mail: org@mail.ifmo.ru

For a solution of a problem of choosing information protection facilities (IPF) two approaches are offered: the first one is based on the assessment of competitiveness, the second one is based on the assessment of the advisability of their using for a particular object of protection. We made review of the methods which evaluate competitiveness of the IPF. The most appropriate methods are: the first - finding of an integral index of the competitiveness, the second – expert evaluations, the third - testing method. For assessment of advisability of using the IPF for a particular object of protection two methods were developed: the method of determining the coefficient of threats neutralization and the method of risk analysis. The method of determining the coefficient of threats neutralization is subjective and based on expert evaluation. The method based on risk analysis assumes the determination of economic benefit from using IPF. Besides, the decision on choosing optimal set of information protection facilities for a particular object is based on the input intensities of information assets.

Key words: information asset, information protection facilities (IPF), risk of information security, object of protection, model of threats, coefficient of threats neutralization, economic efficiency ratio, input intensities of information assets, risk involved.

Развитие информационных технологий привело к тому, что обладание ценной информацией является одним из ключевых факторов успешного ведения бизнеса. Вместе с тем появляется всё большая необходимость в защите информации, доступ к которой ограничен. Вопрос выбора средств защиты информации из всего их многообразия является проблемой для многих предприятий. Часто можно наблюдать ситуации, когда выделенные на защиту информации денежные ресурсы не используются должным образом и, как следствие, не окупаются.

Цель исследования – разработка методов обоснования целесообразности выбора средств защиты информации.

Средства защиты информации (СЗИ) – это технические, программные, программно-технические средства, предназначенные или используемые для защиты информации [2]. Для принятия решения о выборе СЗИ предлагается использовать два подхода: первый основан на сравнительной оценке и определении уровня конкурентоспособности, второй предполагает оценку целесообразности использования СЗИ для конкретного объекта защиты. В работе исследовались оба подхода.

Первый подход. Для оценки конкурентоспособности СЗИ лучше всего подходят три известных метода: метод, основанный на нахождении интегрального показателя конкурентоспособности, метод экспертных оценок и метод тестирования.

Интегральный показатель конкурентоспособности – это обобщенная численная характеристика конкурентоспособности товара, которая рассчитывается по формуле [5]:

$$К_И = \frac{К_Т \cdot К_Ф \cdot К_Н}{К_З}, \qquad (1)$$

где $К_И$ – интегральный показатель конкурентоспособности;

$К_Т$ – коэффициент технической прогрессивности;

$К_Ф$ – коэффициент функциональных возможностей;

$К_Н$ – коэффициент соответствия нормативам;

$К_З$ – коэффициент затрат.

Коэффициенты $К_Т$, $К_Ф$ и $К_З$ находятся путём сравнения технических, функциональных и стоимостных показателей оцениваемого средства защиты информации с аналогичными показателями СЗИ конкурента, принятого за базу. Коэффициент $К_Н$ определяется в зависимости от того, насколько оцениваемое СЗИ соответствует установленным стандартам и нормативам и может принимать значения от 0,5 до 1.

Преимущество метода – учитывается ряд важных факторов, влияющих на уровень конкурентоспособности СЗИ. Недостатки – можно неправильно выбрать параметры для сравнения; не всегда есть возможность получить необходимую информацию о СЗИ.

Сущность метода экспертных оценок состоит в определении ряда технических, экономических и прочих параметров и присвоении СЗИ оценок по каждому из них [1]. Показатель конкурентоспособности определяется по формуле:

$$Ксзи = \sum_{l=1}^{h} I_l \cdot \beta_l, \qquad (2)$$

где $К_{СЗИ}$ – показатель конкурентоспособности средства защиты информации;

I_l – балльная оценка *l*-го параметра;

β_l – коэффициент весомости *l*-го параметра;

h – количество оцениваемых параметров.

Для того чтобы выяснить, насколько мнения экспертов согласованы между собой, находится коэффициент конкордации Кендалла по следующей формуле:

$$W = \frac{12 \cdot S}{f^2 \cdot (h^3 - h)}, \quad (3)$$

где W – коэффициент конкордации Кендалла;

S – сумма квадратов отклонений рангов каждого эксперта от средней суммы рангов;

f – количество экспертов;

Для проверки значимости находится критерий Пирсона (χ^2):

$$\chi^2 = f \cdot (h - 1) \cdot W . \quad (4)$$

Полученное значение критерия Пирсона сравнивается с табличным значением $\chi^2_{кр}$. Если $\chi^2 > \chi^2_{кр}$, то мнения экспертов значимы.

Преимущества метода экспертных оценок – в его простоте и возможности проводить сравнительную оценку при небольшом количестве исходных данных. Главный недостаток заключается в том, что результат полностью зависит от субъективного мнения экспертов.

Тестирование СЗИ может рассматриваться как отдельный метод оценки конкурентоспособности. Объект защиты, охраняемый СЗИ, специально подвергается атакам, либо эти атаки имитируются. Определяется количество или процент успешно отражённых атак. Тестирование чаще всего используется для сравнительной оценки программного обеспечения, например, антивирусов.

Анализ конкурентоспособности позволяет получить сравнительную оценку средств защиты информации для общего случая.

Второй подход. Для того чтобы получить результаты для конкретного потребителя, необходимо провести *оценку целесообразности выбора и использования СЗИ*, которая заключается в определении того, насколько они соответствуют потребностям предприятия в обеспечении информационной безопасности. Для этого предлагается использовать два метода.

Первый метод оценки целесообразности выбора и использования СЗИ для конкретного объекта защиты основан на определении коэффициента нейтрализации угроз и базируется на экспертных оценках. Он состоит из трёх этапов.

Этап 1. Характеристика объекта защиты

Определяется объект защиты, включающий в себя информацию, носители информации и информационные процессы, которые необходимо защищать. В качестве

объекта защиты может быть выбран отдельный компьютер, корпоративная сеть, помещение, предприятие и т.д.

Этап 2. Построение модели угроз

В зависимости от размера предприятия, численности персонала, охраняемой информации, используемых средств и методов защиты, описания типового нарушителя и прочих факторов отбираются существующие угрозы и угрозы, которые могут возникнуть. Эксперты определяют вероятность реализации каждой i-ой угрозы:

$$p_{ri} = p_{ti} \cdot p_{vi}, \quad (5)$$

где p_{ri} – вероятность реализации i-ой угрозы;

p_{ti} – вероятность возникновения i-ой угрозы;

p_{vi} – вероятность возникновения уязвимости для реализации i-ой угрозы.

После этого экспертами определяется относительная оценка потерь (доля ущерба) в случае реализации i-ой угрозы – d_i, которая может принимать значения от 0 до 1.

Для каждой угрозы определяется уровень значимости, равный произведению вероятности её реализации на относительную оценку потерь:

$$z_i = p_{ri} \cdot d_i, \quad (6)$$

где z_i – уровень значимости угрозы.

Этап 3. Определение коэффициента нейтрализации угроз

Выбирается, характеризуется, исследуется и, по возможности, тестируется оцениваемое СЗИ. Экспертами определяется оценка уровня противодействия СЗИ каждой i-ой угрозе – a_i, которая представляет собой целое число в интервале от 0 до 10.

Коэффициент нейтрализации угроз определяется по формуле:

$$К_{НУ} = \frac{\sum_{i=1}^{n} a_i \cdot z_i}{a_{max} \cdot \sum_{i=1}^{n} z_i}, \quad (7)$$

где a_{max} – максимальное значение оценки, равное 10;

n – количество угроз.

На основании полученных результатов можно, во-первых, сделать выбор в пользу средства защиты информации с наибольшим значением коэффициента нейтрализации угроз, а во-вторых, принять решение о целесообразности использования СЗИ. Шкала для принятия решения может выглядеть следующим образом:

- $К_{НУ} < 0{,}05$ – СЗИ нецелесообразно использовать;
- $0{,}05 \leq К_{НУ} < 0{,}2$ – СЗИ компенсирует небольшую часть угроз и может использоваться как дополнительное;

- $0{,}2 \leq К_{НУ} < 0{,}5$ – СЗИ частично компенсирует угрозы и может использоваться вместе с другими СЗИ;
- $0{,}5 \leq К_{НУ} < 0{,}8$ – СЗИ в большей степени компенсирует угрозы и может использоваться как основное, вместе с которым рекомендуется использовать дополнительные СЗИ;
- $0{,}8 \leq К_{НУ}$ – СЗИ рекомендуется к использованию в качестве основного; дополнительные СЗИ могут использоваться по желанию.

Плюсы данного метода в том, что он достаточно прост и не требует сложных расчетов, минусы – субъективность полученного результата и отсутствие стоимостной оценки объекта защиты и средств защиты информации.

Второй метод оценки целесообразности выбора и использования СЗИ для конкретного объекта защиты предполагает определение экономической выгоды от внедрения СЗИ на основе анализа рисков информационной безопасности. Он состоит из пяти этапов.

Этап 1. Определение стоимости информационных активов

Различают два вида активов [4]:

- первичные активы (бизнес-процессы и действия, информация);
- активы поддержки (аппаратные средства, программное обеспечение, сеть).

Для каждого из активов определяется стоимость s_j, которая зависит от затрат на создание или покупку актива, а также возможной выгоды от его использования [4]. Стоимость всех активов складывается, образуя стоимость объекта защиты $S_{ОЗ}$.

Этап 2. Определение перечня актуальных угроз

Составляется перечень угроз, которые существуют или могут возникнуть. После этого строится матрица угроз и активов размерностью n на m, где n – количество угроз, m – количество активов. Для каждой i-ой угрозы по отношению к j-му активу определяется вероятность реализации p_{rji}.

Этап 3. Расчёт цены полного риска

Для каждого актива рассчитывается вероятность реализации хотя бы одной угрозы:

$$p_{rj} = 1 - \prod_{i=1}^{m}(1 - p_{rji}), \qquad (8)$$

где p_{rj} – вероятность реализации хотя бы одной угрозы j-му активу.

Предполагается, что в случае реализации для j-го актива хотя бы одной из угроз, ущерб равняется стоимости актива:

$$q_j = s_j. \qquad (9)$$

Это достигается за счёт детализации активов и тщательного выбора актуальных угроз.

Считается, что угрозы могут быть реализованы независимо друг от друга. Далее вычисляется цена риска R_j для каждого j-го актива по формуле:

$$R_j = p_{rj} \cdot q_j \,. \qquad (10)$$

Цена полного риска равна сумме цен риска для всех активов:

$$R_{ПОЛН} = \sum_{j=1}^{n} R_j \,. \qquad (11)$$

Этап 4. Расчёт цены остаточного риска после внедрения СЗИ

После внедрения СЗИ процедура расчета цены риска выполняется повторно. Определяется цена остаточного риска $R_{ОСТ}$, которая должна быть меньше цены полного риска $R_{ПОЛН}$.

Этап 5. Оценка эффективности использования СЗИ

Коэффициент экономической эффективности от использования СЗИ вычисляется по формуле:

$$E_{СЗИ} = \frac{R_{ПОЛН} - R_{ОСТ}}{S_{СЗИ}}, \qquad (12)$$

где $S_{СЗИ}$ – затраты на СЗИ, которые включают в себя цену покупки, а также затраты на внедрение. Если $E_{СЗИ} > 1$, то данное СЗИ целесообразно использовать, и напротив, если $E_{СЗИ} \leq 1$ – то нецелесообразно.

Однако на основании полученных значений коэффициента экономической эффективности нельзя определить наиболее оптимальный набор средств защиты информации для конкретного объекта защиты. Для этого необходимо учитывать как затраты на СЗИ, так и цену остаточного риска после их внедрения. Кроме того, нельзя допустить, чтобы затраты на СЗИ превысили стоимость информационных активов, поскольку в таком случае они будут неоправданны. Поэтому авторами предлагается использовать показатель затратоёмкости информационных активов, который находится по формуле:

$$\omega = \frac{S_{СЗИ} + R_{ОСТ}}{S_{ОЗ}}, \qquad (13)$$

где ω – затратоёмкость информационных активов.

Данный показатель определяет, какую часть от стоимости информационных активов составляют суммарные затраты, включающие в себя реальные затраты на СЗИ и ожидаемые затраты от реализации угроз безопасности информации, выраженные в виде цены остаточного риска. Наилучшим вариантом выбора СЗИ из нескольких будет тот, при котором значение затратоёмкости информационных активов будет наименьшим.

Выражение (12) можно разложить на слагаемые и ввести следующие обозначения:

$$\omega = \frac{S_{СЗИ} + R_{ОСТ}}{S_{ОЗ}} = \frac{S_{СЗИ}}{S_{ОЗ}} + \frac{R_{ОСТ}}{S_{ОЗ}} = \varepsilon + k \,, \qquad (14)$$

где ε – затратоёмкость обеспечения безопасности информационных активов;

k – рискоёмкость информационных активов.

Выражение (13) подходит для выбора средств защиты информации, а выражение (12) для обоснования целесообразности их использования. Данный метод универсален, поскольку позволяет вычислять и сравнивать показатели экономической эффективности и затратоёмкости информационных активов для разных средств защиты информации и объектов защиты. Его недостатки – сложно определить цену риска; выводы, основанные на оценке неопределённости, как правило, актуальны не больше года.

Результаты оценки конкурентоспособности и оценки целесообразности использования могут не совпадать, поскольку конкурентоспособность определяется для общего случая, а целесообразность использования – исходя из конкретных особенностей потребителя.

Таким образом, предложенные методы могут служить инструментом для принятия решений о выборе и использовании средств защиты информации для конкретных информационных активов с учётом особенностей деятельности предприятия.

Список литературы

1. Васюхин О. В. Основы ценообразования. – СПб.: СПбГУ ИТМО, 2010. – 56 с.
2. ГОСТ Р ИСО/МЭК 50922-2006 «Защита информации. Основные термины и определения»
3. Ларина И. Е. Экономика защиты информации: Учебное пособие. – М.: МГИУ, 2007. – 92 с.
4. Международный стандарт ИСО/МЭК 27005-2008 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», 70 с.
5. Молочнова К. Н. Доклад «Методы оценки технико-экономических показателей проектов программных средств» / руководитель д-р техн. наук, проф. Попов Ф. А. – Бийск, 2008.

Рецензенты:

Васюхин О. В., д-р экон. наук, профессор, заведующий кафедрой «Прикладной экономики и маркетинга» Национального исследовательского университета информационных технологий, механики и оптики, г. Санкт-Петербург.

Каторин Ю. Ф., д-р в. наук, профессор кафедры «Безопасных информационных технологий» Национального исследовательского университета информационных технологий, механики и оптики, г. Санкт-Петербург.