УДК 004.056

Е. В. Легчекова (e.legchekova@gmail.com),
канд. физ.-мат. наук, доцент

Белорусский торгово-экономический университет потребительской кооперации
г. Гомель, Республика Беларусь

О. В. Титов (olvtitov@gmail.com),
канд. физ.-мат. наук, доцент

Конструкторское бюро системного программирования
г. Гомель, Республика Беларусь

МЕТОД РАСЧЕТА РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье предложен метод расчета риска информационной безопасности, произведено сравнение с указанием критичных недостатков с другими методами.

A method for calculating the information security risk is proposed, comparison with the indication of critical shortcomings with other methods.

Ключевые слова: риск; информационная система; информационная безопасность; метод расчета риска; оценка рисков; информационный актив.

Key words: risk; information system; information safety; risk calculation method; risk assessment; information asset.

Оценка рисков как часть направления информационной безопасности (ИБ) (управления рисками) является существенным инструментом в построении защиты. Процесс оценки рисков предназначен для выявления риска для бизнеса организации и определения мер безопасности, предпринимаемых для снижения риска.

В классическом представлении риск – это вероятность реализации угрозы информационной безопасности. Оценка рисков заключается в моделировании картины наступления неблагоприятных условий посредством учета всех возможных факторов, определяющих риск. С математической точки зрения при анализе рисков такие факторы можно считать входными параметрами. При этом нужно учитывать множество источников информации и неопределенность самой информации. На этапе оценки рисков наибольший интерес представляют непосредственно формулы и входные данные для расчета значения риска.

В статье проанализировано несколько разных методов расчета риска и представлена собственная методика. Целью работы является вывод формулы расчета риска информационной безопасности, позволяющей получить массив актуальных рисков и оценить потери в денежном эквиваленте.

Риск информационной безопасности в классическом виде определяется как функция трех переменных:

- вероятности существования угрозы;
- вероятности существования уязвимости (незащищенности);
- потенциального воздействия.

Если любая из этих переменных приближается к нулю, то полный риск стремится к нулю.

Методы оценки рисков. Согласно ISO/IEC 27001 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования», выбранная методология должна гарантировать, что оценки риска дают сравнимые и воспроизводимые результаты. При этом в стандарте не приводится конкретной формулы расчета [1].

В NIST 800-30 «Risk management guide for information technology systems» приводится следующая классическая формула расчета риска:

$$R = P(t) \cdot S,$$

где R – значение риска;

$P(t)$ – вероятность реализации угрозы информационной безопасности (применяется смесь качественной и количественной шкалы);

S – степень влияния угрозы на актив (цена актива в качественной и количественной шкале).

В итоге вычисляется значение риска в относительных единицах, которое можно ранжировать по степени значимости для процедуры управления рисками информационной безопасности [2].

Согласно ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационные технологии. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий», расчет риска в отличии от стандарта NIST 800-30 «Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology» происходит по следующей формуле:

$$R = P(t) \cdot P(v) \cdot S,$$

где $P(t)$ – вероятность реализации угрозы информационной безопасности;
$P(v)$ – вероятность наличия уязвимости;
S – ценность актива.

В качестве примера значений вероятностей $P(t)$ и $P(v)$ приведена качественная шкала с тремя уровнями (низким, средним и высоким). Для оценки значения ценности актива S представлены числовые значения в интервале от 0 до 4. Сопоставление им качественных значений должна произвести организация, в которой производится оценка рисков информационной безопасности [3].

Согласно BS 7799-2:2005 «Спецификация системы управления информационной безопасностью», уровень риска вычисляется с учетом следующих показателей: ценности ресурса, уровня угрозы и степени уязвимости. С увеличением значений этих параметров риск возрастает. Таким образом, формулу можно представить в следующем виде:

$$R = S \cdot L(t) \cdot L(v),$$

где S – ценность актива (ресурса);
$L(t)$ – уровень угрозы;
$L(v)$ – уровень (степень уязвимости).

На практике вычисление рисков информационной безопасности происходит по таблице позиционирования значений уровня угроз, степени вероятности использования уязвимости и стоимости актива. Значение риска может изменяться в диапазоне от 0 до 8, в результате по каждому активу получается список угроз с различными значениями риска. Стандарт предлагает следующую шкалу ранжирования рисков: низкий (0–2), средний (3–5) и высокий (6–8). Это позволяет определить наиболее критичные риски [4].

Согласно РС БР ИББС-2.2-200 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности», оценка степени возможности реализации угрозы информационной безопасности производится по следующей качественно-количественной шкале: нереализуемая угроза – 0%, средняя – от 21% до 50% и т. д. Определение степени тяжести последствий для разных типов информационных активов предлагается оценивать с использованием качественно-количественной шкалы, т. е. минимальное – 0,5% от величины капитала банка, высокое – от 1,5% до 3% от величины капитала банка [5].

Для выполнения качественной оценки рисков информационной безопасности используется таблица соответствия степени тяжести последствий и вероятности реализации угрозы. Если необходимо произвести количественную оценку, то формулу можно представить в следующем виде:

$$R = P(v) \cdot S,$$

где S – ценность актива (степень тяжести последствий).

Рассмотрев все вышеперечисленные методы оценки рисков в части расчета значения риска информационной безопасности, стоит отметить, что расчет риска производится с использованием значения угроз и ценности актива. Значительным недостатком является оценка стои-

мости активов (размер ущерба) в виде условных значений. Условные значения не имеют единиц измерения, применимых в практике, в частности, не являются денежным эквивалентом. В итоге это не дает реального представления уровня риска, который возможно перенести на реальные активы объекта защиты.

Таким образом, предлагается разделить процедуру расчета риска на следующие этапы:

- вычисление значения технического риска;
- вычисление потенциального ущерба.

Под техническим риском понимается значение риска информационной безопасности, состоящего из вероятностей реализации угроз и использования уязвимостей каждого компонента информационной инфраструктуры с учетом уровня их конфиденциальности, целостности и доступности. Для первого этапа можно привести следующие формулы:

$$Rc = Kc \cdot P(T) \cdot P(V);$$

$$Ri = Ki \cdot P(T) \cdot P(V);$$

$$Ra = Ka \cdot P(T) \cdot P(V),$$

где Rc – значение риска конфиденциальности;
Kc – коэффициент конфиденциальности информационного актива;
$P(T)$ – вероятность реализации угрозы;
$P(V)$ – вероятность использования уязвимости;
Ri – значение риска целостности;
Ki – коэффициент целостности информационного актива;
Ra – значение риска доступности;
Ka – коэффициент доступности информационного актива.

Применение данного алгоритма позволит произвести более детальную оценку риска, получить в итоге безразмерное значение вероятности возникновения риска компрометации каждого информационного актива в отдельности.

В последующем возможно вычисление значения ущерба. Для этого используется усредненное значение риска каждого информационного актива и размер потенциальных потерь. Значение ущерба (L) рассчитывается по следующей формуле:

$$L = Rcp \cdot S,$$

где Rcp – среднее значение риска;
S – потери, усл. ед.

Предложенная методика позволяет корректно оценить значение риска информационной безопасности и скалькулировать денежные потери в случае возникновения инцидентов безопасности.

Список использованной литературы

1. **Информационные** технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования : ISO/IEC 27001. – Введ. 06.01.2005. – М. : Стандартинформ, 2006. – 54 с.

2. **Risk** management guide for information technology systems. Recommendations of the National Institute of Standards and Technology : NIST 800-30. – Введ. 06.01.2002. – США. – 2002. – 56 с.

3. **Информационные** технологии. Методы и средства обеспечения безопасности. Ч. 3. Методы менеджмента безопасности информационных технологий : ГОСТ Р ИСО/МЭК ТО 13335-3-2007. – Введ. 01.09.2007. – М. : Стандартинформ, 2007. – 76 с.

4. **Спецификация** системы управления информационной безопасностью : BS 7799-2:2005. – Введ. 01.07.2005. – Англия. – 2005. – 86 с.

5. **Обеспечение** информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности : РС БР ИББС-2.2-200. – Введ. 06.01.2009. – М. : Стандартинформ, 2009. – 23 с.