УДК 004.056

**В.М. Нечунаев**

# Оценка рисков информационной безопасности корпоративной информационной системы

Приведено описание метода оценки рисков информационной безопасности корпоративной информационной системы. С учетом среды функционирования системы производится определение исходных данных, необходимых для процедуры оценки, определение вида величины риска как выходного параметра и описывается алгоритм оценки риска в целом.

**Ключевые слова:** риск, информационная система, информационная безопасность, угроза, ущерб.

Актуальность и необходимость применения процедур оценки и управления рисками информационной безопасности неуклонно возрастает в связи с повышением роли информационных технологий в процессах функционирования организаций как хозяйствующих субъектов.

**Корпоративная информационная система (КИС)** определяется как система, состоящая из персонала, информации и комплекса средств автоматизации, реализующая информационную технологию установленных функций. Исходя из определения, в КИС можно выделить три основных компонента:

- инфраструктура информационных технологий;
- информационные ресурсы;
- персонал и сторонние организации.

КИС является частным случаем социотехнической системы (СЦС). В связи с природой СЦС ее функционирование характеризуется некоторым уровнем неопределенности. Поэтому вопросы оценки уровня безопасности и оценки рисков отличаются для технических и социотехнических систем.

Существующий подход к оценке рисков формулируется следующим образом: риск есть функция от трех входных переменных (вероятности угрозы, уязвимости, ущерба). Рассмотрим данный подход применительно к КИС как СЦС.

Анализ источников угроз, воздействующих на типовую КИС, позволяет выделить четыре типа источников угроз:

- природные;
- техногенные;
- человеческие преднамеренные;
- человеческие непреднамеренные.

Природный тип источника угрозы можно рассматривать в рамках математической вероятностной модели. Для данного типа источника угроз имеется достаточная статистическая база, которая ведется на государственном уровне.

Техногенный тип источника угрозы также можно рассматривать в рамках математической вероятностной модели (поток отказов как инциденты информационной безопасности). Однако не для всех видов технических средств возможно формирование моделей надежности. К примеру, для программных средств сложно формировать модели, определяющие надежность функционирования.

«Человеческий преднамеренный» тип источника угрозы нельзя рассматривать в рамках вероятностной модели. У данного типа угроз обязательно имеется мотивация для деструктивных действий, и поэтому такие действия нельзя рассматривать как случайные. Для оценки данного вида угроз используются игровые модели. Другим вариантом оценки угрозы является использование экспертных оценок на основе косвенных факторов, отражающих потенциальную заинтересованность данного типа источника угрозы в нанесении ущерба активам.

«Человеческий непреднамеренный» тип источника угрозы, с одной стороны, носит случайный характер, с другой стороны, действия данного типа источника угрозы характеризуются высоким уровнем неопределенности. Оценка угрозы производится с использованием методов анализа надежности человеческого фактора [1].

Таким образом, в ходе анализа источников угроз установлено, что не все угрозы КИС носят вероятностный характер. Поэтому понятие риска как функции от вероятности угрозы требует переосмысления.

Рассмотрим понятия «уровень угрозы», «уровень уязвимости», «уровень ущерба», «уровень риска».

1) Уровень угрозы – мера актуальности угрозы.

2) Уровень уязвимости – мера «простоты» использования уязвимости.

3) Уровень ущерба – мера значимости актива для организации.

4) Уровень риска – есть функция $f$ (уровень угрозы, уровень уязвимости, уровень ущерба).

Уровень угрозы определяет меру активности источника угрозы по отношению к КИС/элементам КИС. В связи с различной природой источников угроз информация об их активности может быть представлена количественными либо качественными значениями.

Уровень уязвимости отражает простоту использования уязвимости (необходимые ресурсы источника угрозы) и слабости в защитных мерах. Данный параметр задается по качественной шкале. Использование количественных шкал не представляется возможным ввиду отсутствия или сложности составления математических моделей уязвимостей.

Уровень ущерба определяет возможные последствия для организации/миссии организации в случае наступления инцидента ИБ и является многокритериальной величиной (ущерб репутации, финансовый ущерб, невозможность выполнения миссии организации и т.п.). Интегрированный показатель уровня ущерба определяется по качественной шкале как максимальное значение из критериев, полученное в результате сравнения данных критериев методом анализа иерархий.

Алгоритм оценки риска основывается на методах нечеткой логики и теории нечетких множеств, что позволяет учесть неопределенности, присущие КИС. Общие положения алгоритма оценки рисков:

1) определяются наборы лингвистических термов, характеризующих значения входных параметров (уровень угрозы УУ1, уровень уязвимости УУ2, уровень ущерба УУ3) и выходного параметра (уровень риска УР);

2) задается набор входных параметров $YY1_i$ $(i = 1...M)$, определяющих уровни угроз. Входные параметры имеют количественные значения [0...1] или качественные значения, выраженные в термах лингвистических переменных;

3) задается набор входных параметров $YY2_i$ $(i = 1...N)$, определяющих уровни уязвимостей. Входные параметры имеют качественные значения, выраженные в термах лингвистических переменных;

4) задается набор входных параметров $YY3_i$ $(i = 1...K)$, определяющих уровни ущерба. Входные параметры имеют количественные значения [0...1] или качественные значения, выраженные в термах лингвистических переменных;

5) находится выходной параметр УР, определяющий уровень риска;

6) формируется набор продукционных правил вида "ЕСЛИ, ..., ТО", отражающих взаимосвязи входных параметров с выходным;

7) производится фазификация входных параметров – нахождение значений функций принадлежности, соответствующих полученным значениям оценок входных переменных;

8) производится агрегирование – определение степени истинности условий по каждому из продукционных правил;

9) производится аккумулирование заключений – нахождение функции принадлежности выходного параметра с учетом агрегирования;

10) производится дефазификация выходного параметра.

Таким образом, представленный подход к оценке рисков информационной безопасности позволяет:

– производить оценку уровня риска применительно к КИС как СЦС;

– производить оценку уровня риска как в общем, так и по различным критериям (например, риск потери репутации, финансовый риск, риск на соответствие различным нормам и т.д.).

*Литература*

1. ГОСТ Р 51901.5–2005. Менеджмент риска. Руководство по применению методов анализа надежности. – М.: Стандартинформ, 2005. – 71 с.

2. Зырянова Т.Ю. Модель системы управления информационной безопасностью в условиях неопределенности воздействия дестабилизирующих факторов: автореф. дис. ... канд. техн. наук. – Томск, 2008. – 25 с.

3. Шумский А.А., Системный анализ в защите информации / А.А. Шумский, А.А. Шелупанов. – М.: Гелиос АРВ, 2005. – 224 с.

**Нечунаев Вадим Михайлович**
Ижевский государственный технический университет,
каф. «Системы и технологии информационной безопасности», аспирант.
Отделение Пенсионного фонда Российской Федерации
(государственное учреждение) по Удмуртской Республике,
ведущий специалист-эксперт отдела защиты информации

V.M. Nechunaev
**Information security risk assessment for corporate information system**
In the present article the description of information security risk assessment method for corporate information system is resulted. In view of system environment definition of the initial data indispensable for procedure of an assessment is made,definition of type of risk size as target parameter is made and the risk assessment algorithm is described.
**Keywords:** risk, information system, information security, threat, damage.