УДК 004.056

К вопросу об определении угроз и рисков информационной безопасности с использованием сценарного подхода и факторного планирования эксперимента

П. В. Плетнев, В. М. Белов, Е. В. Зубков, О. А. Крыжановская

В работе рассматриваются существующие методы для оценки вероятностей угроз и рисков информационной безопасности (ИБ). Представлена обобщённая схема оценки рисков ИБ. На примере внедрения внутренним нарушителем вредоносного кода рассматривается применение сценарного подхода и факторного планирования эксперимента для оценки вероятностей реализации угроз ИБ.

Ключевые слова: информационная безопасность (ИБ), защита информации (ЗИ), определение вероятностей угроз, оценка рисков, информационная система (ИС), факторное планирование эксперимента (ФПЭ).

1. Введение

Для создания эффективной системы ЗИ необходимо определить актуальные угрозы и проанализировать риски ИБ. Данной тематике в настоящее время уделяется большое внимание: научные исследования и различные методики описывают разнообразные подходы к оценке угроз и рисков ИБ.

В общем случае оценка угроз представляет собой один из этапов анализа рисков ИБ. Оценка рисков производится на основе данных о вероятности реализации возможных угроз и потенциальных последствиях. Современные методики анализа рисков ИБ можно классифицировать в зависимости от используемого подхода к оценке угроз ИБ: качественные, количественные, комбинированные [1].

Количественные методы оценки базируются на использовании математического аппарата для определения вероятностей реализации угроз. Широко применяются инструменты теории множеств, теории вероятностей, теории шансов, дискретной математики и т.д. [2]. Рассматриваемая группа методов позволяет формализовать процесс оценки угроз, снизить субъективизм экспертов и наглядно представить результаты анализа рисков ИБ. Однако для получения объективного результата предварительно необходимо собрать точные сведения, характеризующие возможность реализации угроз и экономическую целесообразность построения системы ЗИ: данные о частоте реализации угроз; принятые меры защиты, их стоимость и эффективность; стоимость активов и потенциальные потери и т.д. Недостаток данных препятствует получению адекватных оценок, поэтому такие подходы следует применять на этапе разработки ИС. Использование данных методов требует высокого уровня подготовки экспертов и значительных временных затрат.

Качественные методы оценки являются более популярными по сравнению с количественными ввиду возможности моделирования различных сценариев реализации угроз ИБ. Исследование и совершенствование данных методов широко распространено среди зарубеж-

ных авторов, их основой послужили общепризнанные стандарты ISO и BS. Качественные методы оценки оперируют не числовыми значениями, а эквивалентными им ранжированными показателями. Определение вероятностей реализации угроз осуществляется в соответствии с принятой шкалой. Использование таких подходов позволяет упростить и одновременно ускорить процесс оценивания угроз, но существует проблема получения противоречивых или недостоверных конечных результатов вследствие субъективности и некомпетентности экспертов.

Комбинированный подход включает в себя принципы количественных и качественных методов, совмещая экспертное оценивание вероятностей угроз ИБ с анализом на основе статистических данных. Такое комбинирование позволяет применять данные методы на практике, не требуя от специалистов высокой квалификации, а также снизить субъективное влияние экспертов на результаты анализа рисков ИБ.

В настоящей работе представлена общая схема оценки рисков ИБ и проведена оценка вероятности реализации угроз с использованием сценарного подхода и ФПЭ на примере угрозы внедрения вредоносного кода внутренним нарушителем.

2. Общая схема оценки рисков ИБ

В настоящей работе приводится расширенный вариант схемы оценки рисков ИБ (рис. 1), представленной в статье [3]. В обновлённой схеме предложено одновременно выявлять уязвимости и анализировать принятые меры защищённости, что позволит дать более точную оценку исходному состоянию ИС. В расширенном варианте схемы оценивания рисков ИБ учтены возможные способы обработки рисков, а также предусмотрена оценка остаточных рисков и последующий контроль эффективности принятых мер.

Согласно схеме (рис. 1) на 1-м этапе определяются характеристики ИС: ресурсы, ценность активов, проводится их категоризация и т.д. На 2-м этапе выявляются уязвимости и параллельно проводится анализ принятых мер защищённости для их нейтрализации.

На 3-м этапе, опираясь на данные, полученные на предыдущем этапе, идентифицируются потенциальные угрозы ИБ, характерные для существующих брешей в СЗИ.

На 4-м этапе осуществляется параллельная оценка вероятностей реализации угроз ИБ и их возможных последствий. На 5-м этапе на основе данных, полученных на предыдущем этапе, определяются риски ИБ. На 6-м этапе осуществляется выбор способа обработки рисков ИБ и их анализ. Существует четыре возможных способа анализа рисков: принятие (сохранение), уменьшение, передача, избежание [4].

На 7-м этапе производится оценка остаточных рисков, анализируется результативность принятых мер, в случае если результат неудовлетворительный, осуществляется возврат к обработке рисков. На 8-м этапе оформляется отчёт об анализе рисков. На 9-м этапе проводится мониторинг новых потенциальных угроз и своевременная переоценка рисков ИБ, поскольку организация и поддержание безопасности ИС представляет собой непрерывный процесс.

Зачастую в ходе анализа рисков возникают затруднения при определении вероятностей реализации угроз. По причине недостаточности статистических данных о реализации угроз нередко оценка вероятностей базируется на экспертном мнении. Метод оценки вероятностей угроз ИБ на основе ФПЭ, предложенный в работе [5], позволяет уменьшить субъективизм экспертов при решении данной проблемы.

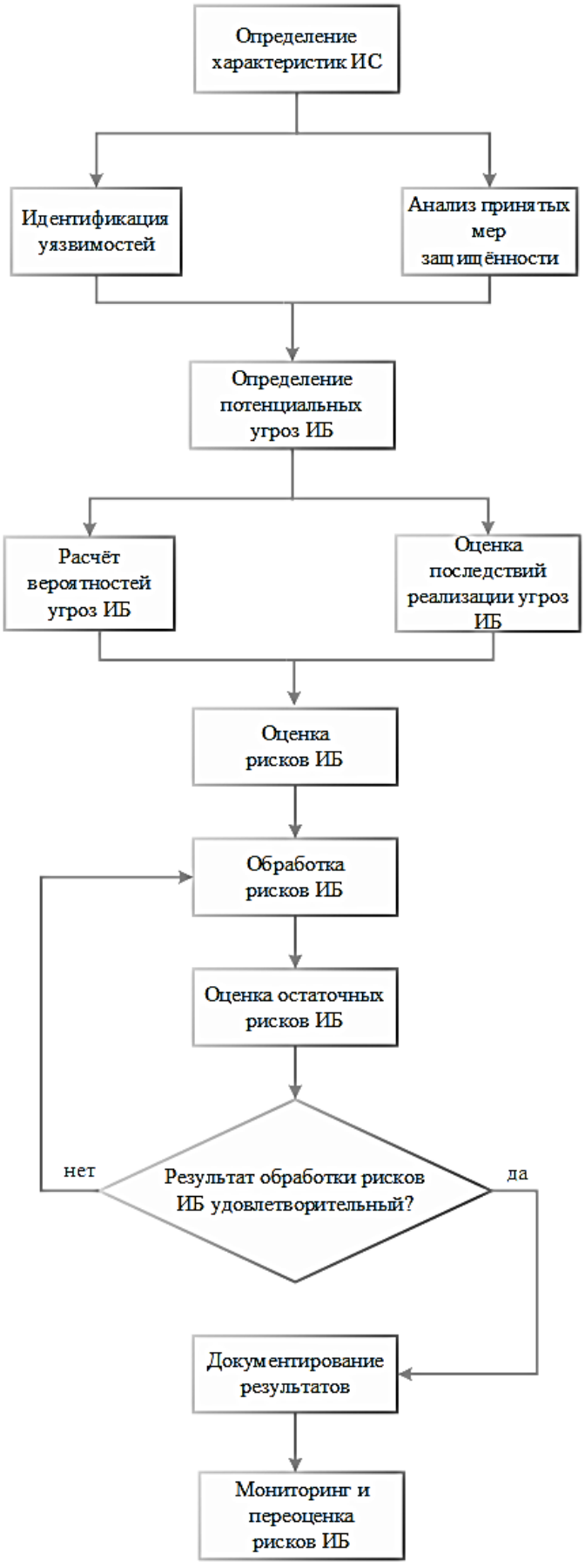

Рис. 1. Общая схема оценки рисков ИБ

3. Метод оценки вероятностей угроз ИБ на основе ФПЭ

Планирование эксперимента – это процедура выбора числа условий, необходимых и достаточных для получения математической модели процесса [6]. В ходе планирования эксперимента необходимо определить количество опытов, в контексте оценки вероятностей угроз ИБ опыт представляет собой возможный сценарий их реализации. Под сценарием подразумевается совокупность факторов рисков (X_1, X_2, ..., X_k), способствующих успешной реализации угроз ИБ. Факторы рисков способствуют реализации угроз как по одному, так и в совокупности. Эксперимент, учитывающий все возможные сценарии, называется полнофакторным. Количество сценариев в данном случае определяется следующим образом:

$$\boldsymbol{N = m^k}, \tag{1}$$

где N – количество экспериментов, m – число уровней факторов, k – количество факторов. Поскольку в данной модели факторы могут принимать одно из двух значений – 0 или 1 в зависимости от степени влияния на реализацию угрозы (т.е. фактор либо оказывает влияние, либо нет), формула (1) принимает следующий вид:

$$\boldsymbol{N = 2^k}. \tag{2}$$

Математическая модель полнофакторного эксперимента представляет собой уравнение регрессии:

$$\boldsymbol{Y = b_0 + \sum_{i=1}^{k} b_i * X_i + \sum_{\substack{i,j=1 \\ i \neq j}}^{k} b_{ij} * X_i * X_j + \cdots + \sum_{\substack{i,j,\ldots,n \neq 1 \\ i \neq j \neq \cdots \neq n}}^{k} b_{ijn} * X_i * X_j * X_n}, \tag{3}$$

где Y – вероятность реализации угрозы, X_i – значения факторов, b_0 – свободный член, b_i – коэффициент линейного воздействия факторов, b_{ij} – коэффициент взаимодействия факторов, b_{ijn} – коэффициент n-го взаимодействия факторов.

Модель полнофакторного эксперимента применяют в случае, когда число факторов не превышает трёх. При большем количестве экспериментов, как правило, применяют модель дробного факторного эксперимента, что позволяет упростить расчёты за счёт сокращения количества сценариев и коэффициентов регрессии. Для осуществления перехода в формуле (3) выбирают незначительные взаимодействия (как правило, коэффициенты взаимодействия, начиная с тройных, незначимы) и присваивают их менее важным факторам.

В ходе планирования эксперимента строится матрица планирования, отражающая информацию о сценариях. Значения факторов вносятся в неё в следующем виде: 1 заменяют на +1, 0 – на -1, для облегчения восприятия 1 в матрице опускается. В столбцы, отражающие взаимодействие факторов, вносят произведения соответствующих вектор-столбцов. После определения возможных сценариев эксперты ранжируют их в зависимости от потенциальной опасности по шкале от 0.00 до 1.00. При оценивании сценариев важно присваивать им уникальные значения.

После заполнения матрицы планирования осуществляется расчёт коэффициентов регрессии. Линейные коэффициенты находят по формуле:

$$\boldsymbol{b_j = \frac{\sum_{i=1}^{N} X_{ji} * Y_i}{N}, j = 0, 1, 2, \ldots, k}, \tag{4}$$

где N – количество опытов, j – номер фактора, X – значение фактора, Y– значение оценки вероятности реализации сценария. Коэффициенты взаимодействия определяются аналогично линейным коэффициентам. Коэффициенты для уравнения регрессии полнофакторного эксперимента вида 2^3 рассчитываются по формулам (5) – (8):

$$\boldsymbol{b_{12}} = \frac{\sum_{i=1}^{N}(X_1X_2)_i * Y_i}{N}, \quad (5)$$

$$\boldsymbol{b_{13}} = \frac{\sum_{i=1}^{N}(X_1X_3)_i * Y_i}{N}, \quad (6)$$

$$\boldsymbol{b_{23}} = \frac{\sum_{i=1}^{N}(X_2X_3)_i * Y_i}{N}, \quad (7)$$

$$\boldsymbol{b_{123}} = \frac{\sum_{i=1}^{N}(X_1X_2X_3)_i * Y_i}{N}. \quad (8)$$

Таким образом можно получить оценки вероятностей реализации угроз ИБ.

4. Оценка вероятности реализации угрозы внедрения вредоносного кода внутренним нарушителем

Пусть реализации данной угрозы способствуют следующие факторы:

X_1 – устаревшие антивирусные базы,

X_2 – отсутствие запрета на запуск исполняемых файлов от имени пользователей,

X_3 – возможность управления функционированием антивирусного программного обеспечения от имени пользователей,

X_4 – возможность установления удалённого подключения к персональному компьютеру.

По формуле (2) находим, что эксперимент будет состоять из 16 сценариев. Для упрощения вычислений осуществим переход к дробному факторному планированию эксперимента, пренебрегая незначимыми взаимодействиями, начиная с тройных. Для фактора X_4 используем вектор-столбец $X_1X_2X_3$, тогда уравнение регрессии принимает следующий вид:

$$\boldsymbol{Y = b_0 + b_1X_1 + b_2X_2 + b_3X_3 + b_4X_4 + b_{12}X_1X_2 + b_{13}X_1X_3 + b_{23}X_2X_3}. \quad (9)$$

Матрица планирования эксперимента представлена в таблице 1.

Таблица 1. Матрица планирования эксперимента

№	X_0	X_1	X_2	X_3	X_4 ($X_1X_2X_3$)	X_1X_2	X_1X_3	X_2X_3	Y
1	+	-	-	-	-	+	+	+	0
2	+	+	-	-	+	-	-	+	0.95
3	+	-	+	-	+	-	+	-	0.87
4	+	+	+	-	-	+	-	-	0.97
5	+	-	-	+	+	+	-	-	0.82
6	+	+	-	+	-	-	+	-	0.96
7	+	-	+	+	-	-	-	+	1.0
8	+	+	+	+	+	+	+	+	0.98

Рассчитав по формулам (5) – (8) коэффициенты регрессии, получаем искомое уравнение регрессии:

$$\boldsymbol{Y = 0.82 + 0.15X_1 + 0.14X_2 + 0.12X_3 + 0.09X_4 - 0.13X_1X_2 - 0.12b_{13}X_1X_3 - 0.09X_2X_3}.$$

5. Заключение

В ходе оценки вероятности внедрения внутренним нарушителем вредоносного кода было установлено, что факторы X_1 и X_2 имеют наибольшее влияние, X_4 – наименьшее. Величина свободного члена регрессии указывает на то, что изменение значения одного из факторов может существенно повлиять на реализацию угрозы. Поскольку значения факторов близки по значимости, то они друг друга существенно не усиливают.

Литература

1. *Белкин С. А., Белов В. М.* Сравнительный анализ методов оценки угроз информационной безопасности // Доклады VI Пленума СибРОУМО по образованию в области информационной безопасности и XV конференции, Томск – Иркутск, 9–13 июня 2014 г. Томск: В-Спектр, 2014. С. 188–194.
2. *Плетнев П. В., Белов В. М.* Сравнительный анализ существующих методов определения рисков информационной безопасности // Ползуновский вестник. 2011. № 3 (1). С. 221–223.
3. *Белкин С. А., Белов В. М., Пивкин Е. Н.* Об общей схеме оценки рисков информационной безопасности // Измерение, контроль, информатизация: материалы XV Международ. науч.-практ. конф. Барнаул: Изд-во АлГТУ, 2014. С. 270–272.
4. *Астахов А. М.* Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 312 с.
5. *Белкин С. А., Белов В. М., Пивкин Е. Н.* Применение факторного планирования эксперимента для оценки вероятностей угроз информационной безопасности // Ползуновский вестник. 2014. № 2. С. 232–234.
6. *Белкин С. А., Белов В. М.* Оценка вероятности угрозы заражения компьютерным вирусом на основе факторного планирования эксперимента // Информационное противодействие угрозам терроризма. 2014. № 23. С. 55–61.

Статья поступила в редакцию 20.01.2016

Плетнев Павел Валерьевич
генеральный директор ООО «Центр информационной безопасности Алтайского края», тел. +7-923-655-03-00, e-mail: ppv@secret-net.ru.

Белов Виктор Матвеевич
д.т.н., профессор, профессор кафедры безопасности и управления в телекоммуникациях СибГУТИ, тел. +7-906-963-84-83, e-mail: vmbelov@mail.ru.

Зубков Евгений Валерьевич
аспирант кафедры безопасности и управления в телекоммуникациях СибГУТИ, тел.+7-913-798-01-48, e-mail: evz.nsk@gmail.com.

Крыжановская Ольга Александровна
студент кафедры информационной безопасности НГУЭУ, тел. (383) 224-59-55, e-mail: krizanovskaya@ngs.ru.

On the definition of threats and risks of information security with the scenario approach and factorial experiment

P. Pletnev, V. Belov, E. Zubkov, O. Kryzhanovskaya

This paper considers existing approaches of definition threats and risks of information security. The generalized scheme of information security risk assessment is presented, and method for evaluating the probability of threats based on scenario planning approach and factorial experiment is considered on the example of the introduction of insider malicious code.

Keywords: data protection, determining the probability of threats, factorial experiment, information security, information system, risk assessment.