РАЗДЕЛ 6. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056

ПРИМЕНЕНИЕ ФАКТОРНОГО ПЛАНИРОВАНИЯ ЭКСПЕРИМЕНТА ДЛЯ ОЦЕНКИ ВЕРОЯТНОСТЕЙ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.А. Белкин, В.М. Белов, Е.Н. Пивкин

В статье рассматривается задача оценки угроз информационной безопасности (ИБ). Предложен алгоритм процедуры расчета вероятностей угроз на основе факторного планирования эксперимента

Ключевые слова: информационная безопасность, модель, полный факторный эксперимент (ПФЭ), дробный факторный эксперимент (ДФЭ).

Актуальность

Одним из этапов оценки рисков ИБ является получение вероятностей реализации угроз. Несмотря на большое многообразие методов, методик и алгоритмов оценки рисков, вопрос о разработке новых подходов остается открытым [1].

В работе [2] была предложена общая схема оценки рисков ИБ. На наш взгляд, эта схема имеет ряд серьезных недостатков.

Согласно предложенной схеме эксперты должны составить список актуальных угроз, а затем рассчитать риски. Это не совсем верно, потому что эксперты судят об актуальности тех или иных угроз после получения информации о наличии тех или иных рисков.

Оценка эффективности организационных и технических мер защиты должна проводиться одновременно с расчетом вероятностей реализации угроз. В связи с этим мы предлагаем придерживаться следующей общей схемы оценки рисков (см. рисунок) [3].

На этапе 1 определяем характеристики информационной системы (ИС): ресурсы, информационные потоки и т.д., составляющие эту систему.

На этапе 2 составляем список уязвимостей ИС и соответствующих им угроз.

В ходе этапа 3 осуществляем анализ мер безопасности, которые уже были внедрены, и которые планируется внедрить, чтобы не допустить возникновения новых рисков.

На этапе 4 определяем вероятности реализации угроз.

Следующим важным этапом (этап 5) при оценке рисков является определение величины ущерба при потере конфиденциальности, целостности или доступности в результате успешной реализации угроз.

На этапе 6, используя полученные на предыдущих этапах оценки вероятностей и ущербов, определяем риски ИБ. Как известно, риск представляет собой произведение вероятности угрозы на величину соответствующего ущерба [4]:

$R = P \cdot S$,

где P – вероятность угрозы,

S – нанесенный ущерб.

На этапе 7 определяем меры безопасности, которые подходят для снижения рисков.

На этапе 8 составляем отчет об оценке рисков.

Этапы 4 и 5 можно проводить параллельно после того, как будет завершен первый этап.

В данной работе предлагаем способ создания модели оценки вероятностей реализации угроз на основе факторного планирования эксперимента. Такая модель позволяет сократить число этапов в схеме, изложенной в публикации [2] и, таким образом, повысить качество оценки рисков.

Построение модели оценки вероятностей угроз с помощью факторного планирования эксперимента

Планирование эксперимента - это процедура выбора числа условий необходимых и достаточных для получения математической модели процесса.

Для простоты эксперимента модель будет представлять собой функцию регрессии, которая показывает зависимости вероятностей угроз от различных факторов:

$$y = b_0 + \sum_{i=1}^{k} b_i \cdot x_i + \sum_{\substack{i,j=1 \\ i \neq j}}^{k} b_{ij} \cdot x_i \cdot x_j + \ldots + \sum_{\substack{i,j,\ldots,n=1 \\ i \neq j \neq \ldots \neq n}}^{k} b_{ijn} \cdot x_i \cdot x_j \cdot \ldots \cdot x_n . \quad (1)$$

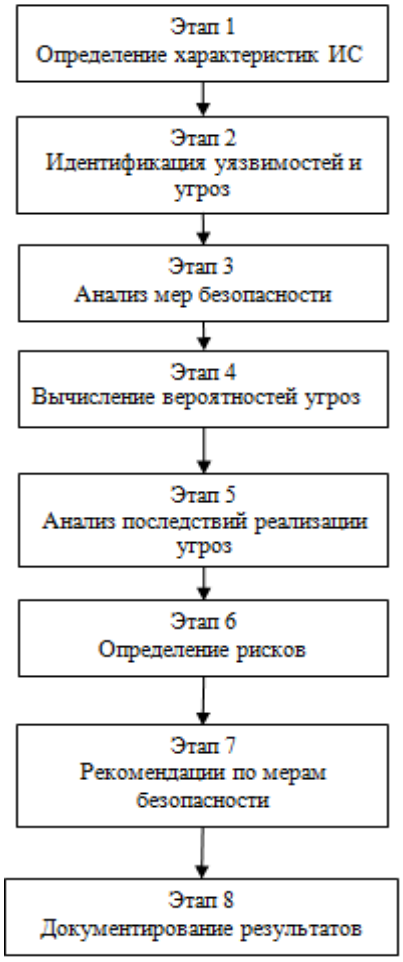

Рисунок - Общая схема оценки рисков ИБ

Здесь x_i – кодированное значение фактора, y – вероятность реализации угрозы, b_0 - свободный член, b_i - коэффициент линейного воздействия фактора, b_{ij} - коэффициент парного взаимодействия факторов и b_{ijn} - коэффициент n-го взаимодействия факторов.

Под фактором понимают проявление уязвимости или любое другое событие, которое может повлиять на значение вероятности угрозы. Факторы, как по одному, так и в совокупности, вносят свой вклад в реализацию угрозы. Уровень или значение, которое может принимать фактор равно 1 или 0, т.е. фактор либо вносит свой вклад, либо не вносит. В нашей работе факторы назовем факторами рисков. Чтобы проще было составить список уязвимостей, угроз и факторов, удобно воспользоваться стандартами в области ИБ.

Вместо опытов будем формулировать сценарии угроз, затем эксперты зададут точечные оценки каждому сценарию по шкале от 0.00 до 1.00. Шкала показывает степень опасности каждого сценария по сравнению с другим. При этом учитываем мотивацию и возможности источника угроз, а также эффективность принятых мер защиты.

Чем больше факторов, тем больше сценариев требуется рассмотреть. Если число факторов равно двум или трем, то планирование эксперимента можно осуществить по схеме ПФЭ. В этом случае число сценариев находим по формуле

$$N = 2^k, \qquad (2)$$

где k – количество факторов рисков.

Если факторов больше трех, то проводить планирование эксперимента лучше по схеме ДФЭ. Последняя позволит сократить количество сценариев и коэффициентов регрессии (1). Для этого в (1) необходимо выбрать незначительные взаимодействия (коэффициенты взаимодействия, начиная с тройных и выше, часто незначимы, поэтому ими можно пренебречь) и присвоить их менее важным факторам.

В процессе планирования эксперимента эксперты строят матрицу планирования, куда заносят информацию о сценариях. Значения факторов при этом кодируют. Единицу заменяют на +1, 0 - на -1. Обычно единицу можно опустить и оставить «+» или «-».

После составления матрицы планирования и получения данных, переходим к следующему этапу – расчету коэффициентов регрессии. Коэффициенты вычисляем по формуле [5]:

$$b_j = \frac{\sum_{i=1}^{N} x_{ji} \cdot y_i}{N}, j = 0,1,2,\ldots,k. \qquad (3)$$

В этой формуле N – количество сценариев, j – номер фактора, x – кодированное значение фактора и y – значение вероятности угрозы.

Коэффициенты взаимодействия определяем аналогично линейным коэффициентам. Так для ПФЭ с тремя факторами коэффициенты находим таким образом

$$b_{12} = \frac{\sum_{i=1}^{N} (x_1 x_2)_i y_i}{N}, b_{13} = \frac{\sum_{i=1}^{N} (x_1 x_3)_i y_i}{N},$$
$$b_{23} = \frac{\sum_{i=1}^{N} (x_2 x_3)_i y_i}{N}, b_{123} = \frac{\sum_{i=1}^{N} (x_1 x_2 x_3)_i y_i}{N}. \qquad (4)$$

В результате, можно получить модель оценки реализации угроз.

Отсюда, процедура создания модели оценки вероятностей угроз состоит из следующих этапов:

Алгоритм

1. Формулирование факторов рисков;
2. Построение матриц планирования экспериментов и определение общего вида функций регрессий;
3. Заполнение матриц данными о сценариях угроз;
4. Расчет коэффициентов регрессий по формулам (3) и (4).

Вычислительный эксперимент

Предположим, на некотором предприятии Z требуется оценить вероятность проникновения в помещение, где располагается ИС. На реализацию угрозы могут повлиять следующие факторы рисков:

1. X_1 - выход из строя электронного замка;
2. X_2 - выход из строя видеокамер;
3. X_3 – инсайдер, который может сообщить о неисправностях замка, видеокамер сообщнику;
4. X_4 – сотрудник, который может случайно пропустить злоумышленника в помещение, где располагается ИС.

Теперь проведем планирование эксперимента. По формуле (2) получаем, что ПФЭ будет состоять из 16 опытов и уравнение регрессии примет вид:

$$y = b_0 + b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4 + b_{12}x_1x_2 + b_{13}x_1x_3 + b_{14}x_1x_4 + b_{23}x_2x_3 + b_{24}x_2x_4 + b_{34}x_3x_4 + b_{123}x_1x_2x_3 + b_{124}x_1x_2x_4 + b_{134}x_1x_3x_4 + b_{234}x_2x_3x_4 + b_{1234}x_1x_2x_3x_4.$$

Чтобы упростить задачу воспользуемся ДФЭ. В этом случае эксперимент будет состоять из 8 опытов, а уравнение регрессии иметь вид

$$y = b_0 + b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4 + b_{12}x_1x_2 + b_{13}x_1x_3 + b_{23}x_2x_3.$$

Матрицу факторного планирования представим таблицей.

После проведенных вычислений получаем искомое уравнение регрессии:

$$y = 0.5 + 0.0375x_1 + 0.0625x_2 + 0.385x_3 + 0.0125x_4.$$

В полученное уравнение регрессии следует подставлять кодированные значения факторов. Если фактор вносит вклад, то его значение равно 1, иначе - -1.

Результаты планирования эксперимента показывают, что фактор X_3 не только вносит наибольший вклад в реализацию угрозы, но и усиливает негативное действие других факторов. ИБ является непрерывным процессом, а не разовым мероприятием, поэтому служба безопасности должна осуществлять постоянный мониторинг факторов рисков на предмет их изменений, а также появления новых факторов.

Таблица - Матрица планирования эксперимента

№	X_0	X_1	X_2	X_3	X_1X_2	X_1X_3	X_2X_3	X_4 $(X_1X_2X_3)$	y
1	+	-	-	-	+	+	+	-	0
2	+	+	-	-	-	-	+	+	0.1
3	+	-	+	-	-	+	-	+	0.15
4	+	+	+	-	+	-	-	-	0.2
5	+	-	-	+	+	-	-	+	0.8
6	+	+	-	+	-	+	-	-	0.85
7	+	-	+	+	-	-	+	-	0.9
8	+	+	+	+	+	+	+	+	1.0

СПИСОК ЛИТЕРАТУРЫ

1. Плетнев, П.В. Сравнительный анализ существующих методов определения рисков информационной безопасности [Текст] / П.В. Плетнев, В.М. Белов // Ползуновский вестник. - 2011. - №3/1. - С. 221 - 223.
2. Плетнев, П.В. Общая схема и обобщенный алгоритм оценки угроз и рисков информационной безопасности [Текст] / П.В. Плетнев, В.М. Белов, Е.Н. Пивкин // Надежность функционирования и информационная безопасность телекоммуникационных систем железнодорожного транспорта: Материалы всероссийской научно-технической интернет-конференции с международным участием. – Омск: ОмГУПС, 2013. - С.205-209.
3. Петренко, С.А. Управление информационным и рисками. Экономически оправданная безопасность [Текст] / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи, 2004, - 384 с.: ил.
4. Грибунин, В.Г. Комплексная система защиты информации на предприятии [Текст]: учеб. пособие для студ. высш. учеб. заведений / В.Г. Грибунин, В.В. Чудовский. – М.: Издательский центр «Академия», 2009. – 416 с.
5. Любченко, Е.А. Планирование и организация эксперимента [Текст]: учебное пособие. Часть 1. / Е.А. Любченко, О.А. Чуднова. - Владивосток: Изд-во ТГЭУ, 2010. - 156 с.

Аспирант ***Белкин С.А.,*** *serega-box2011@yandex.ru – Новосибирский государственный университет экономики и управления, каф. информационной безопасности; д.т.н., проф.* ***Белов В.М.*** *vmbelov@mail.ru - Сибирский государственный университет телекоммуникаций и информатики, каф. безопасности и управления в телекоммуникациях; к.т.н., специалист* ***Пивкин Е.Н.****, evpiv@yandex.ru – Управление ФНС России по Московской области.*