УДК [004.056.5+004.413.4]:519.234

В. В. Мохор[1], В. В. Цуркан[2]
[1]Институт проблем моделирования в энергетике им. Г.Е. Пухова
Национальной академии наук Украины
ул. Генерала Наумова, 15, 03164, Киев-164, Украина
[2]Институт специальной связи и защиты информации
Национального технического университета Украины «КПИ»
ул. Московская, 45/1, 01011, Київ-011, Украина

Количественная оценка рисков безопасности информации на основе пробит-анализа

Приведено обоснование постановки задачи развития методологии количественной оценки рисков безопасности информации конкретных объектов информационной деятельности на основе пробит-анализа.

Ключевые слова: *пробит-анализ, пробит-функция, безопасность информации, риск, количественная оценка рисков, анализ рисков.*

В настоящее время наличие систем управления безопасностью информации становится одним из ключевых условий стратегического развития любой организации. В соответствии со стандартом ISO/IEC 27001:2005 [1] определение требований к разработке, внедрению, применению, мониторингу, анализу, поддержанию и улучшению системы управления информационной безопасностью должно осуществляться в контексте менеджмента рисков безопасности информации конкретной организации. Основным и наиболее сложным этапом управления рисками безопасности информации является анализ рисков.

Для анализа рисков безопасности информации существуют различные методики, а именно: Austrian IT Security Handbook, AS/NZS4360, BSI 100-3, CRISAM, EBIOS, HB167:200X, ISF IRAM, ISO 27005:2008, ISO 31000, MAGERIT, MARION, MEHARI, NIST SP800-30, OCTAVE, OSSTMMRAV, SOMAP и другие. Выбор той или иной методики зависит от уровня требований, предъявляемых в организации к обеспечению безопасности информации, характера принимаемых во внимание угроз и эффективности мер по защите информации [2].

Согласно [3] задача анализа рисков безопасности информации разделяется на две стадии:

— идентификацию рисков (*Risk Identification*);

— оценку рисков (*Risk Estimation*).

В настоящей работе нас интересует задача оценки рисков, которая согласно [3] предполагает:

— определение метода оценки рисков, причем оценка, в свою очередь, может быть:

– качественной;

– количественной;

— оценку последствий инцидентов информационной безопасности;

— определение характеристик вероятности (случайности) инцидентов информационной безопасности;

— вычисление уровня риска.

В [4] выделено четыре подхода к количественной оценке риска, различаемых по исследуемым сферам его проявления. Применительно к безопасности информации целесообразно рассмотреть технократический подход, основанный на анализе относительных частот возникновения опасных явлений с нежелательными последствиями. Методология количественной оценки рисков основывается на вероятностях исходных событий, сценариях развития инцидентов с возможными последствиями и соответствующими вероятностями их реализации. В соответствии с этой методологией возможны следующие методы количественной оценки рисков [4, 5].

1. Статистические методы — предполагается определение вероятности реализации угрозы для рассматриваемого информационного актива за интервал времени на основе выполнения следующих требований:

— объекты, к анализу которых предполагается использовать статистику, и объекты, на которых собрана статистика, являются эквивалентными (требование эквивалентности объектов);

— условия, при которых предполагается использовать статистику, и условия ее сбора являются эквивалентными (требование эквивалентности условий);

— объемы выборок статистики являются достаточными, методы обработки — корректными, а источники сведений — заслуживающими доверия (требование убедительности).

К недостаткам этой группы методов следует отнести критичность к исходным данным, которые, как правило, или отсутствуют, или их недостаточно для построения корректных выводов.

2. Вероятностно-статистические методы используют привлечение дополнительной информации о распределении ущербов в случае реализации угрозы безопасности информационного актива. Предполагается, что для рассматриваемых условий функционирования организационно-технической системы предприятия известна функция распределения ущерба инцидентов информационной безопасности. На ее основе определяется доля катастрофических событий от общего числа негативных событий. Считая эту долю постоянной либо прогнозируя по временному ряду ее значение на заданный момент времени, можно определить вероятностные характеристики катастрофических событий.

При этом точность и достоверность результатов, полученных с применением вероятностно-статистических методов, определяется качеством и объемом дополнительной информации о распределении ущербов.

3. Теоретико-вероятностные методы используются для определения частот или вероятностей реализации редких угроз безопасности информации со значительными последствиями, по которым статистика практически отсутствует. В основе этого метода лежат закономерности перерастания инициирующих событий в чрезвычайные, декомпозиция задачи, оценки частных показателей и определение частоты редких негативных событий с учетом взаимосвязи частных показателей.

Теоретико-вероятностный метод достаточно трудоемок, имеет низкую точность и достоверность получаемых в процессе исследования результатов, но при отсутствии других оценок его применение оправдано.

4. Экспертные методы основываются на знаниях и опыте экспертов. Эти методы целесообразно применять в том случае, когда отсутствуют статистические данные. При этом экспертам предлагается ответить на вопросы о состоянии или будущем поведении информационных активов, характеризующихся неопределенными параметрами или неизученными свойствами. Для интерпретации или математической обработки экспертных данных можно использовать математический аппарат теории нечетких множеств.

Сложность анализа рисков безопасности информации экспертным методом связана, прежде всего, с неопределенностью характеристик массивов данных, на базе которых сформирован опыт эксперта и, как следствие, с отсутствием гарантий получения достоверных результатов.

Таким образом, можно констатировать наличие существенных ограничений в применении известных методов количественной оценки рисков в сфере безопасности информации, в связи с чем поиск новых подходов, обеспечивающих решение задач определения характеристик вероятности (случайности) безопасности информации в условиях недостаточных статистик, представляет собой актуальную задачу.

В этом контексте представляется перспективным рассмотреть возможность пробит-анализа, идея которого принадлежит американскому энтомологу Ч. Блиссу, впервые описавшего ее в статье о влиянии пестицидов на процент уничтоженных вредителей [6, 7]. Ч. Блисс предложил для учета процента уничтоженных вредителей использовать вероятностный блок — «**prob**ability un**it**» или «probit» («пробит)». Сначала необходимость введения понятия «пробит» была обусловлена стремлением избежать работы со статистической информацией. В то время биологи, для которых и предназначался этот метод, были мало ознакомлены со статистической обработкой результатов эксперимента. В настоящее время эта причина утратила свое значение, однако, названия «пробит» и «пробит-анализ» стали привычными терминами, методология «пробит-анализа» получила свое развитие и широко применяется в токсикологии, фармакологии, радиобиологии, энтомологии, экологии и других областях как биологических, так и медицинских исследований [8].

Суть пробит-анализа состоит в специальном отображении *S*-подобных кривых зависимости потерь от характеристик реализованных угроз в прямые линии, которые в дальнейшем могут быть обработаны методами линейного анализа. Обратное преобразование осуществляется путем преобразования значений линейных пробит-функций в значения характеристик вероятности.

Известно [8], что пробит-функция есть математическая зависимость, которая связывает специфические особенности негативного воздействия на некоторый объект (в нашем случае — информационный актив) с размером возможных потерь. Выражение для определения значений пробит-функции в общем случае, имеет следующий вид:

$$\Pr(D) = a + b\ln D + \gamma \ln \tau,$$

где a, b, γ — коэффициенты, которые характеризуют степень уязвимости информационного актива в отношении конкретной угрозы либо класса угроз; D — оценка негативного воздействия; τ — период времени от начала до конца негативного воздействия.

Для сфер, в которых можно пренебречь временным периодом актуальности угрозы, а именно это и характерно для большинства случаев угроз безопасности информации, используется следующая форма представления пробит-функции:

$$\Pr(D) = a + b\ln D. \tag{1}$$

На основе аналогии с функциями распределения вероятностей потерь от реализации сценариев угроз безопасности информации с *S*-подобными кривыми следует предположить, что использование подхода на основе пробит-анализа может оказаться результативным.

При этом необходимо отметить, что решение задачи определения вероятностных характеристик для каждой пары (угроза, уязвимость) выполняется в два этапа:

1) определение значений элементов пробит-функции $\Pr(D)$, входящих в правую часть выражения (1);

2) расчет пробит-функции $\Pr(D)$ и определение по известным значениям пробит-функции значений вероятностных характеристик.

Начнем рассмотрение задачи с конца, т.е. со второго этапа. Пусть значения величин a, b, D известны. Тогда, в соответствии с выражением (1), можно рассчитать значение пробит-функции $\Pr(D)$. Согласно [8], по известным $\Pr(D)$ вычисляются значения вероятности реализации угрозы безопасности информации по следующей формуле:

$$P = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\Pr(D)} e^{-\frac{x^2}{2}} dx, \tag{2}$$

где пробит-функция $\Pr(D)$ выступает верхним пределом интегрирования, а само выражение (2) уже не содержит эмпирических коэффициентов.

На практике для вычисления интеграла (2) применяют таблицу значений пробит-функции [8], использование которой поясним на примере.

Значения пробит-функции

P, %	0	1	2	3	4	5	6	7	8	9
0		2,67	2,95	3,12	3,25	3,38	3,45	3,52	3,59	3,66
10	3,72	3,77	3,82	3,86	3,92	3,96	4,01	4,05	4,08	4,12
20	4,16	4,19	4,23	4,26	4,29	4,33	4,36	4,39	4,42	4,45
30	4,48	4,50	4,53	4,56	4,59	4,61	4,64	4,67	4,69	4,72
40	4,75	4,77	4,80	4,82	4,85	4,87	4,90	4,92	4,95	4,97
50	5,00	5,03	5,05	5,08	5,10	5,13	5,15	5,18	5,20	5,23
60	5,25	5,28	5,31	5,33	5,36	5,39	5,41	5,44	5,47	5,50
70	5,52	5,55	5,58	5,61	5,64	5,67	5,71	5,74	5,77	5,81
80	5,84	5,88	5,92	5,95	5,99	6,04	6,08	6,13	6,18	6,23
90	6,28	6,34	6,41	6,48	6,55	6,64	6,75	6,88	7,05	7,33
–	0,0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
99	7,33	7,37	7,41	7,46	7,51	7,68	7,65	7,75	7,88	8,09

Предположим, необходимо найти вероятность реализации угрозы безопасности информации по известному значению пробит-функции, $\Pr(D) = 4{,}53$. Данному значению соответствует пересечение строки «30 %» и столбца «2 %» таблицы, при котором вероятность реализации угрозы безопасности информации равна 32 %. К тому же, возможна ситуация, когда пробит-функция принимает средние значения, например: $\Pr(D) = 4{,}515$. В этом случае вероятность реализации угрозы безопасности информации может быть определена с помощью следующего выражения:

$$P(4{,}515) = \frac{P(4{,}53) + P(4{,}50)}{2} = \frac{32\ \% + 31\ \%}{2} = \frac{63\ \%}{2} = 31{,}5\ \%.$$

Таким образом, второй этап решения задачи оценки значений вероятности при количественной оценке рисков безопасности информации на основе подхода с использованием пробит-анализа можно считать предопределенно выполненным.

Рассмотрим теперь первый этап задачи — определение значений элементов пробит-функции $\Pr(D)$, входящих в правую часть выражения (1). Из этого выражения видно, что нахождение значений $\Pr(D)$ для конкретной угрозы или класса угроз безопасности информации предполагает определение значений коэффициентов *a, b* и величины *D*. При этом непосредственно из выражения (1) следует, что коэффициент *a* отражает уровень постоянных затрат, необходимых для поддержания безопасности заданного актива, а *b* представляет собой коэффициент «усиления» потерь *D*, обусловленных результативным развитием сценария актуализации угрозы безопасности информации.

Согласно [9] можно указать два альтернативных способа определения значений *D*:

1) значения *D* определяются в виде отношения

$$D = \frac{h}{H},$$

где h — величина потерь (затрат) на ликвидацию последствий активности конкретной угрозы в отношении конкретного информационного актива; H — максимальные потери (затраты), возможные вследствие реализации угроз безопасности информации для данного объекта;

2) значение D определяется на основании результатов анализа параметров угроз и уязвимостей. Например, в [10, 11] приведены результаты исследований по определению значений D для инцидентов на гидротехнических сооружениях. Если методику [11] интерпретировать в контексте безопасности информации, то, в частности, получим, что значение D определяется в виде произведения некоторого коэффициента опасности $\lambda_{on.}$ на некоторый коэффициент уязвимости v_y:

$$D = \lambda_{on.} \cdot v_y ,$$

(здесь и далее мы сохраняем обозначения, принятые в [11]). При этом:

$$\lambda_{on.} = \lambda_0 \sum_{i=1}^{M} \delta_i \cdot a_i , \tag{3}$$

$$v_y = v_0 \sum_{j=1}^{N} \varphi_j \cdot a_j , \tag{4}$$

где λ_0 и v_0 — нормирующие множители, значения которых выбираются, исходя из условий:

$$0 < \lambda_{on.} \le 1 ,$$
$$0 < v_y \le 1 .$$

Из выражений (3) и (4) видно, что коэффициент опасности $\lambda_{on.}$ и коэффициент угрозы v_y определяются в виде суммы M или, соответственно, N показателей a_i или a_j. В соответствии со стандартом [3], идентификация показателей угроз и уязвимостей осуществляется в процессе анализа рисков. При этом численные значения показателей a_i и a_j устанавливаются, например, в баллах на основе их упорядочения и ранжирования, проводимого, например, методом анализа иерархий [12]. Для сглаживания/усиления степени влияния отдельных показателей каждому из них может ставиться в соответствие параметр значимости δ_i (или φ_j) выбираемый в диапазоне (0, 1) при соблюдении условия:

$$\sum_{i=1}^{M} \delta_i = 1$$

либо

$$\sum_{j=1}^{N} \varphi_j = 1$$

соответственно. Выбор одного из двух способов определения значений величины *D* зависит от выбранной методики анализа рисков [3]. Если методика приоритетно ориентирована на анализ потерь, то следует выбирать первый способ. Если же методика отдает приоритет анализу угроз и уязвимостей, то следует предпочесть второй способ.

Наибольшая неопределенность связана с определением значений коэффициентов *a* и *b* для сферы безопасности информации. В целом, установление значений этих коэффициентов для каждой пары угроза/последствие осуществляется в результате проведения отдельных исследований. В частности, такие исследования проведены, например, в энтомологии, экологии, токсикологии, фармакологии, радиобиологии и других областях биологических и медицинских наук. Известны примеры таких исследований в гидротехнике, строительной механике, пожарной безопасности и других сферах, отличных от информационной безопасности. Вместе с тем, анализ и идентификация особенностей и характеристик, как угроз безопасности информации, так и уязвимостей, присущих различным информационным активам, является рекомендацией стандарта [3] и нормативным требованием стандарта [1]. В настоящее время выполнение таких исследований для каждой из организаций и по каждому из активов является практически невыполнимым, как в силу разнообразия условий и контекста их функционирования, так и в силу динамики этих условий во времени. Использование же подхода, состоящего в построении пробит-функций, обеспечивает единую методологическую базу учета особенностей пар угроза/последствие для различных информационных активов и создает основу для решения задачи количественной оценки рисков в сфере безопасности информации.

При этом развитие методологии пробит-анализа применительно к сфере безопасности информации может рассматриваться в качестве отдельного, самостоятельного направления научных исследований.

1. ISO/IEC 27001:2005. Information Technology. — Security Techniques. — Information Security management Systems. — Requirements.

2. *Петренко С.А.* Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. — М.: Компания АйТи; ДМК Пресс, 2004. — 384 с.

3. ISO/IEC 27005:2005. Information technology. — Security Techniques. — Information Security Risk Management.

4. *Вишняков Я.Д.* Общая теория рисков: учеб. пособие для студ. высш. учеб. заведений/ Я.Д. Вишняков, Н.Н. Радаев. — 2-е изд., испр. — М.: Издательский центр «Академия», 2008. — 368 с.

5. *Буянов В.П.* Рискология (управление рисками): учеб. пособие / В.П. Буянов, К.А. Кирсанов, Л.М. Михайлов. — 2-е изд., испр. и доп. — М.: Экзамен, 2003. — 382 с.

6. *Bliss C.I.* The Method of Probits / C.I. Bliss // Science. — 1934. — Vol. 79, N 2037. — P. 38–39.

7. *Bliss C.I.* The Method of Probits — A Correction / C.I. Bliss // Science. — 1934. — Vol. 79, N 2053. — P. 409–410.

8. *Белов П.Г.* Системный анализ и моделирование опасных процессов в техносфере: учеб. пособие для студ. высш. учеб. Заведений / Петр Григорьевич Белов. — М.: Издательский центр «Академия», 2003. — 512 с.

9. *Методические* рекомендации по оценке риска аварий гидротехнических сооружений, водохранилищ и накопителей промышленных отходов / [Куранов Н.П., Розанов Н.Н. и др.]. — М.: ЗАО «ДАР/ВОДГЕО», 2002. — 44 с.

10. *Куранов Н.П.* Интегральный метод оценки риска аварий гидротехнических сооружений / Н.П. Куранов, Н.Н. Розанов, Е.А. Тимофеева // Сб. науч. тр. по материалам 8-го Международного конгресса «Вода: экология и технология», ЭКВАТЭК-2008, М., 3–6 июня 2008 г.

11. *Методические* рекомендации по оценке риска аварий гидротехнических сооружений водохранилищ и накопителей промышленных отходов: Рекомендации [Электронный ресурс]: от 14.08.2001, № 9-4/02-644 / Государственный комитет РФ по строительству и жилищно-коммунальному комплексу. — 2001. — Режим доступа: http://www.businesspravo.ru/Docum/DocumShow_DocumID_141332_DocumIsPrint_Yes_Page_.html. — Дата доступа: сентябрь 2010. — Название с экрана.

12. *Саати Т.* Принятие решений. Метод анализа иерархий / Т. Саати. — М.: Издательство «Радио и Связь», 1993. — 278 с.

Поступила в редакцию 13.09.2010