УДК [004.056.5+004.413.4]::519.234 **Мохор В.В., Цуркан В.В.**

ПРОБИТ-АНАЛИЗ РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

На сегодняшнее время, наличие системы управления безопасностью информации является одним из необходимых условий стратегического развития любой организации. При этом, определение требований по разработке, внедрению, применению, мониторингу, анализу, поддержанию и улучшению системы управления информационной безопасностью осуществляется в ***контексте рисков*** конкретной организации [1]. Следует отметить, что под риском в настоящей работе будем понимать риск безопасности информации («information security risk»). Как следствие, в организации необходимо определить методику построения оценок риска, которая должна соответствовать установленным требованиям к защите информации и позволять получить сравнимые и воспроизводимые результаты.

Для построения оценок риска 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 одной из них 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 построения оценок риска включает в себя два этапа. При этом, одним из основных этапов является анализ рисков безопасности информации, который служит отправной точкой для установления и поддержки эффективного управления системой безопасности информации. Кроме этого потребность анализа рисков обусловлена, прежде всего, необходимостью, во-первых, описания состава и структуры организационно-технической системы, во-вторых, ранжирования информационных активов по приоритетам с учетом степени их значимости, а, в-третьих, выявления угроз и уязвимостей информационных активов. К тому же, анализ рисков безопасности информации направлен на достижение следующих основных целей [3, 4]:

– формирование перечня информационных активов с учетом их значимости в пределах установленной границы управления риском безопасности информации;

– формирование перечня угроз с определением их вида и источника;

– формирование перечня существующих и планируемых средств контроля, их нахождение и состояние использования;

– формирование:

а) перечня угроз, связанных с информационными активами, угрозами и средствами контроля;

б) перечня угроз, не связанных с подлежащей рассмотрению определенной угрозой;

– формирование перечня сценариев инцидентов с их последствиями, которые связанны с информационными активами.

В [4] выделено четыре концепции анализа риска, различаемых по исследуемым сферам его проявления. Применительно к безопасности информации, целесообразно рассмотреть технократическую концепцию, которая основана на анализе относительной частоты возникновения опасных явлений с нежелательными последствиями. Так, при оценке риска рассматриваются вероятности исходных событий, сценарии их развития с соответствующими вероятностями реализации и возможными последствиями.

Рассмотрим области применения методов анализа рисков безопасности информации в соответствии с технократической концепцией [4, 5, 6]:

1. Статистические методы – определение вероятности реализации угрозы для рассматриваемого информационного актива за интервал времени, осуществляется с помощью статистических данных, которые получаются при использовании следующих способов:

а) увеличение интервала наблюдения за предшествующие годы;

б) расширение совокупности исследуемых информационных активов, в равной степени подверженных рассматриваемому риску.

К недостаткам методики следует отнести зависимость от значительного объема данных, которые, как правило, отсутствуют или их недостаточно для анализа рисков безопасности информации.

2. Вероятностно-статистические методы – основанные на привлечении дополнительной информации о распределении ущербов в случае реализации угрозы безопасности информационного актива. Исходя из этих соображений, предполагается, что для рассматриваемых условий функционирования организационно-технической системы организации известно распределение негативных событий по ущербу. После этого 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 построить методику анализа вероятности катастрофического события.

При этом точность и достоверность результатов полученных с применением теоретико-вероятностной методики определяется качеством и объёмом дополнительной информации о распределении ущербов.

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

Теоретико-вероятностный метод достаточно трудоемок и 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. Этот метод 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, во-первых, с отсутствием гарантий получения точных и достоверных результатов анализа, а, во-вторых, с трудностью проведения экспертного опроса и обработки полученных данных.

Из обзора методов анализа рисков следует:

1. Выбор адекватного метода анализа рисков определяется имеющимся объемом статистических данных, а также видом дополнительной информации о распределении ущерба вследствие реализации угрозы безопасности информации.

2. Точность и достоверность результатов анализа рисков зависти от общего числа наблюдений и числа реализовавшихся негативных событий.

3. С учетом пунктов 1 и 2 сложно получить объективные результаты анализа показателя риска, который выражается вероятностью реализации угрозы безопасности информации.

В связи с этим, целью настоящего исследования является пробит-анализ рисков безопасности информации в условиях недостаточного объема исходной информации. При этом вероятность потерь *Prob* выражается через пробит-функцию *Pr(D)* следующим образом

$$\mathrm{Prob} = f[\mathrm{Pr}(D)],$$

где величина *D* – «оценка негативного воздействия».

Обозначенная цель достигается путем решения следующих задач:

1. Определить значения пробит-функции для конкретной угрозы либо класса угроз безопасности информации.

2. Определить значение вероятностей потерь, возможных вследствие реализации угроз безопасности информации.

Заметим, что идея использования пробит-анализа уже известна [7]. Она принадлежит американскому энтомологу Ч. Блиссу. В 1934 г. он описал ее в статье о влиянии пестицидов на процент убитых вредителей. Ч. Блисс предложил для учёта процента убитых вредителей использовать вероятностный блок – «**prob**ability un**it**» или «probit» («пробит)». Пробит-анализ – метод математической статистики, который применяется для обработки *S*-подобных кривых зависимости реализации угроз, например: «угроза реализована – угроза нереализованная», от величины убытков. Использование данного метода позволяет найти величину убытков и оценить вероятность реализации угроз безопасности информации. При этом суть рассматриваемого метода состоит в линеаризации *S*-подобной кривой, путем преобразования ее в прямую линию, которая может быть обработана методами анализа линейной зависимости.

Сначала необходимость введения понятия «пробит» была обусловлена стремлением избежать работы с отрицательными числами. Однако надо иметь в виду, что в то время биологи, для которых и предназначался этот метод, не имели даже простейших счетных машин и были мало ознакомлены со статистической обработкой результатов эксперимента. Поэтому отказ от использования отрицательных величин действительно имел практическое значение. В настоящее время эта причина утратила свое значение, однако, названия «пробит» и «пробит-анализ» стали настолько привычными терминами, что отказ от них мог бы вызвать путаницу, в частности, в использовании табличных данных, поскольку в большинстве таблиц указываются значения пробитов [7]. Окончательно определение понятия «пробит» дал Д. Финни в своей работе «Probit analysis», первое издание которой вышло в 1947 г.

Пробит-анализ нашел свое применение в токсикологии, фармакологии, радиобиологии, энтомологии, экологии и других областях как биологических, так и медицинских исследований. При этом попытка анализа рисков безопасности информации з позиций пробит-метода авторами предпринята впервые.

Прежде чем приступить к определению значений пробит-функции предположим, что множество угроз или множество классов угроз безопасности информации известно. Таким образом, пробит-функция учитывает специфические особенности негативного воздействия (например, атаки в контексте реализации угрозы) на информационный актив и размер возможных убытков от реализации угроз безопасности информации. Выражение для определения значений пробит-функции в общем случае, имеет следующий вид [8]

$$\Pr = a + b\ln D + \gamma \ln \tau, \qquad (1)$$

где a, b, γ і $k = \gamma / b$ – коэффициенты, которые характеризуют степень уязвимости информационного актива от конкретной угрозы либо класса угроз; D – «оценка негативного воздействия»; τ – время между концом и началом негативного воздействия.

При этом в дальнейших исследованиях будем использовать, следующую форму записи (1), которая применяется на практике [8]:

$$\Pr = a + b\ln D. \qquad (2)$$

Решая задачу определения значения пробит-функции для конкретной угрозы или класса угроз безопасности информации, разделим ее на две частных подзадачи, то есть:

1. Определение коэффициентов пробит-функции*, a, b*;
2. Определение «оценок негативного воздействия», *D*.

При этом значения коэффициентов *a, b,* входящих в используемое выражение для аргумента пробит-функции (2) можно найти лишь в иностранной литературе [8]. В контексте данной статьи ограничимся только этим фактом, предполагая, что определение коэффициентов *a* и *b*, характеризующих угрозу или класс угроз, может быть рассмотрено в качестве отдельной задачи исследования.

Применительно к определению «оценок негативного воздействия» *D,* выделим следующие два аспекта:

1. Параметр *D* представляет собой величину ущерба. В этом случае ее значение определяется исходя, например, из:

– затрат на ремонт, например: компьютерной техники, без/с учетом стоимости комплектующих деталей;

– стоимости новой техники, например: компьютерной;

– стоимости восстановления информации в зависимости от объема накопителя, сложности и срочности выполнения работ.

2. Параметр D представляет собой коэффициент риска [9]. Для разъяснения этого тезиса проинтерпретируем результаты анализа параметра D полученные в [10] применительно к задаче анализа рисков безопасности информации. При этом «оценка негативного воздействия» D определяется через значения поражающих факторов.

В качестве количественного показателя опасности примем коэффициент опасности реализации угрозы безопасности информации $\lambda_{on.}$, $0 < \lambda_{on.} < 1$. Определим значение коэффициента опасности реализации угрозы безопасности информации, который вычисляется по следующей формуле:

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

где δ_i – коэффициент значимости *и-того* показателя опасности, a_i – сумма кода *и-того* показателя опасности, λ_0 – нормирующий множитель, который предотвращает выход значений $\lambda_{on.}$ за границы интервала $0 < \lambda_{on.} < 1$.

По аналогии с коэффициентом опасности реализации угрозы безопасности информации, вводится коэффициент уязвимости информационного актива

$$v_y = \sum_{i=1}^{n} \varphi_i \cdot a_i \cdot v_0,$$

де φ_i – коэффициент значимости *и-того* показателя уязвимости информационного актива, a_i – сумма кода *и-того* показателя уязвимости, v_0 – нормирующий множитель, который предотвращает выход значений v_y за границы интервала $0 < v_y < 1$.

Поскольку наибольшая угроза безопасности информации возникает при пересечении двух событий – опасности реализации угрозы и уязвимости информационного актива, целесообразно в качестве оценки негативного воздействия выбрать мультипликативную величину, характеризующую совместное действие всех показателей, то есть

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

После того, как будет определено значение пробит-функции, вычислим вероятность потерь вследствие реализации угрозы безопасности информации. Для решения этой задачи воспользуемся функцией ошибок Гаусса, которую еще называют эрфик-функцией, по следующей формуле [11, 12]:

$$\mathrm{Prob} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\mathrm{Pr}} e^{-\frac{\lambda^2}{2}} d\lambda, \qquad (3)$$

где Pr – пробит-функция, которая является верхним пределом интегрирования эрфик-функции.

При этом следует обратить внимание на то, что выражение (3) не содержит эмпирических коэффициентов и, как следствие, зависимость Prob = f[Pr(D)] можно представить в виде графика либо таблицы для каждой угрозы или класса угроз. К тому же рассматриваемую зависимость можно представить как в виде линии по отношению к своим параметрам, так и с помощью степенного множителя, применение которого упрощает анализ и оценивание рисков безопасности информации. Исходя из этих соображений, пробит-функция применима на практике и имеет достаточно четкое обоснование. При этом она включает все существенные факторы, учитываемые в процессе анализа рисков безопасности информации.

Тем не менее, в процессе пробит-анализа рисков безопасности информации следует иметь ввиду и такие его особенности [7]:

– в литературных источниках неоднозначно определена верхняя граница в формуле (3);

– представление выражения для определения пробит-функции в виде упрощенного двучлена

$$\Pr = a + b \ln D;$$

– неоднозначность толкования «оценок негативного воздействия» D.

Указанные свойства могут приводить к ошибкам прогноза – по причине несоответствия коэффициентов a, b в формулах, используемых для определения значения пробит-функции в разной литературе. В связи с этим, для получения правильного результата при прогнозировании значений вероятности реализации угрозы с помощью пробит-функции целесообразно сначала проверить достоверность соответствующих коэффициентов, а потом убедится в их пригодности к оцениванию конкретных угроз или класса угроз безопасности информации. Это достигается благодаря подставлению параметров a і b в выражение для определения D и вычисление его значения.

Таким образом:

1. В процессе анализа рисков наиболее актуальной является проблема получения информации, во-первых, о вероятностях реализации угроз и, во-вторых, о степени значимости и потенциальных последствиях реализации угроз безопасности информации. Как следствие, ограниченность исходной информации приводит к статистической неопределенности, что чревато возможностью получения ошибочных оценок риска. При этом основная проблема анализа рисков состоит в том, чтобы выявить показатели неопределенности и риска в условиях недостаточного объема исходной информации.

2. Впервые в области управления рисков безопасности информации для их анализа использован пробит-метод. Особенность его применения состоит в том, что в формуле для определения вероятности потерь отсутствуют эмпирические коэффициенты, тем самым, исключается зависимость результатов анализа рисков безопасности информации от объема исходных данных.

Итак, пробит-анализ рисков безопасности информации позволяет одновременно оценить как вероятность реализации угрозы или класса угроз, так и величину ущерба вследствие воздействия на информационные активы с учетом всех влияющих факторов в условиях недостаточного объема исходных данных. При этом следует иметь в виду, что от качественно проведенного анализа рисков безопасности информации в значительной степени зависит, насколько эффективно и надежно в дальнейшем будет функционировать организационно-техническая система и, в конечном итоге, удастся ли рассматриваемому субъекту в достаточной мере защититься от угрожающих ему рисков безопасности информации.

Список літератури

1. *ISO/IEC 27001:2005*. Information technology. – Security techniques. – Information security management systems. – Requirements.
2. *Петренко С.А.* Управление информационными рисками. Экономически оправданная безопасность/Петренко С.А., Симонов С.В. – 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) [Текст] : учеб. пособие / В. П. Буянов, К. А. Кирсанов, Л. М. Михайлов. - 2-е изд., испр. и доп. - М. : Экзамен, 2003. - 382 с.
6. *Живетин В.Б.* Введение в анализ риска [Текст]: монография / *В.Б. Живетин*. – Казань: [б. и.], 1999. - 319 с.
7. *Платонов А.Г., Ахалая М.Я.* Дозовая зависимость постлучевой гибели. Расчет полулетальной дозы LD_{50} методом пробит-анализа. М.: [б.и.], 2006. – 33 с.
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. *Куранов Н. П., Розанов Н. Н. и др*. Методические рекомендации по оценке риска аварий гидротехнических сооружений, водохранилищ и накопителей промышленных отходов. – М.: ЗАО «ДАР/ВОДГЕО», 2002. – 44 с.
10. *Куранов Н.П., Розанов Н.Н., Тимофеева Е.А.* Интегральный метод оценки риска аварий гидротехнических сооружений // Сборник материалов 8-го Международного конгресса «Вода: экология и технология», ЭКВАТЭК-2008, М., 3-6 июня 2008 г.
11. *Аверин Г.В., Звягинцева А.В.* Опасность и риск как характеристики особых состояний экологических и техногенных систем//Екологічна безпека. – 2008. – № 2. – С.22 – 30.
12. *Модели* и методы оценки техногенного ущерба при гуманитарном разминировании [Электронный ресурс] / Л.П. Андреев // Вісник Східноукраїнського національного університету імені Володимира Даля, 2009.- № 5. – Режим доступу: http://www.nbuv.gov.ua/e-journals/vsunud/2009-5E/09alppgr.htm. – Назва з екрану.

Рецензент: д.т.н., проф. Хорошко В.О.
Надійшла 11.03.2010 р.