УДК 519.2

В.В. Мохор, д.т.н., профессор, ИПМЭ им. Г.Е. Пухова НАН Украины, Киев
В.В. Цуркан, ИССЗИ НТУУ «КПИ», Киев

СРАВНЕНИЕ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ЭНТРОПИЙНОГО ПОДХОДА К ОПРЕДЕЛЕНИЮ РИСКА

The approach to an estimation of information security risks safety with use of an entropy of a probability distribution is considered.

На сегодняшний день актуальной задачей является оценка систем информационной безопасности. Как показывает анализ источников [1-4], в качестве количественной оценки потенциальных угроз реализации тех или иных уязвимостей информационных активов, способных нанести вред (ущерб), необходимо оценить «риск информационной безопасности» (или «информационный риск»).

Если говорить о рисках в контексте информационной безопасности, то, например, в [5] приводятся следующие определения:

1. Риск – это вероятная частота и вероятная величина будущих потерь (Метод FAIR).
2. Риск – это сочетание вероятности события и его последствий (ГОСТ Р 51901-2002).
3. Риск – это комбинация вероятности события и его последствий (ГОСТ Р ИСО/МЭК 17799-2005).
4. Риск – это вероятность причинения ущерба вследствие того, что определенная угроза реализуется в результате наличия определенной уязвимости (ГОСТ Р 52448-2005).
5. Риск – это потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов (ГОСТ Р ИСО/МЭК 13335-1-2006; проект ГОСТ Р ИСО/МЭК 13569).

Можно продолжить этот список цитатами из новейших нормативных документов, но в целом картина не изменится: численная оценка информационного риска определятся в виде комбинации двух агрегированных оценок: размера (величины) негативных последствий (ущерба) и вероятности возникновения этого ущерба, т.е. вероятности реализации угрозы.

В настоящем сообщении мы не будем касаться оценок ущерба, а остановимся на анализе другой составляющей – вероятности реализации угрозы. Прежде всего, отметим, что согласно духу международных нормативных документов в сфере менеджмента информационной безопасности информационные риски следует рассматривать относительно активов, а точнее – относительно информационных активов. (Определение

этого понятия вызвало оживленные дебаты, например, по данной теме на форуме сайта http://dom.bankir.ru/ за последние 5 месяцев было зарегистрировано более 200 сообщений и более 5000 просмотров.) Наиболее общее определение информационного актива дано в [6] – это «нечто, обладающее ценностью для организации (например, оборудование, программное обеспечение, данные, люди и документация)», но не только это, ибо, как отмечается в том же источнике, к активу должен быть отнесен, например, имидж фирмы.

Согласно [6] угроза информационной безопасности определяется, как «причина или событие, которые могут оказывать негативное влияние на информационный актив и приводить к потере конфиденциальности, целостности или доступности актива». Т.е. угроза подразумевает два фактора: «причину» и «возможное следствие». Подтверждение и разъяснение этого тезиса находим в документе ФСТЭК РФ «Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПД» от 14.02.2008, а именно: о наличии угрозы свидетельствует «наличие источника угрозы и уязвимого звена, которое может быть использовано для реализации угрозы». Иными словами, угроза представляет собой пару {источник, уязвимость}, каждый из компонентов которой может характеризоваться своими частотными и временными показателями.

Принимая во внимание все многообразие факторов, которые нужно учитывать при оценке информационного риска, следует признать, что неопределенности в этих факторах больше чем статистической определенности. В связи с этим можно предположить, что оценки неопределенности рисков являются более корректными, чем оценки вероятности реализации угрозы. Учитывая, что мерой неопределенности является энтропия, можно предложить использовать энтропийный подход для оценки информационных рисков.

Следует сразу оговориться, что идея использовать энтропию для оценки рисков сама по себе не нова, она высказывалась, например в [7, 8]. Но анализ доступных литературных источников и материалов сети Интернет показал, что эта идея ранее не использовалась другими авторами для решения задач оценки рисков информационной безопасности.

Итак, будем полагать, что для некоторого объекта A априори известно множество из n информационных угроз и упорядоченное множество из m состояний ущерба от реализации этих угроз:

$$h_1, h_2, ..., h_i, ..., h_m.$$

Очевидно, что $m \le n$, т.е. существуют такие угрозы, которые не тождественны между собой, но, тем не менее, приводят к одинаковому ущербу. Например, очевидно, что для защищенных систем существуют угрозы, ущерб от реализации которых равен нулю.

Кроме того, упорядоченность подразумевает, что

$$0 \le h_1 \le h_2 \le \ldots \le h_i \le \ldots \le h_m \le h_{\max},$$

где h_{max} представляет собой ущерб, равный полной ликвидации всех информационных активов объекта за бесконечно малый промежуток времени без каких либо остатков. Будем так же полагать, что нам известно распределение вероятностей p_i по множеству элементов h_i, (отложив пока вопрос о том, на основании чего получено такое распределение и как оно соотносится с объективной реальностью). Это значит, что ущерб h_1 возникает с вероятностью p_1, ущерб h_2 - с вероятностью p_2, ущерб h_i - с вероятностью p_i и т.д.

Кроме того, будем полагать, что события реализации угроз являются независимыми и множество всех событий реализации угроз является полным, т.е.

$$\sum_i p_i = 1$$

Тогда можно определить энтропию

$$H(A) = -\sum_{k=1}^{m} p_k \log p_k ,$$

которую предлагается использовать в качестве оценки риска информационной безопасности объекта A. Корректность этого тезиса подтверждается следующими свойствами энтропии [9]:

1. Величина

$$H(A) > 0 .$$

Это означает, что риск информационной безопасности может быть либо равен нулю, либо быть больше нуля, но не может быть отрицательным. В этом состоит отличие рисков безопасности от коммерческих рисков, где может существовать отрицательный риск, который эквивалентен доходу в противовес ущербу при положительном риске. (Возможно именно по этой причине энтропийный подход не нашел широкого распространения в оценке финансовых рисков.)

2. Если объекты A и B независимы, то

$$H(AB) = H(A) + H(B) .$$

Из этого следует, что риск информационной безопасности двух объектов равен сумме рисков каждого из объектов, что согласуется с интуитивным представлением о риске информационной безопасности.

3. Если объекты A и B имеют одинаковые распределения вероятностей ущерба, то риск информационной безопасности для таких объектов одинаков.

4. Если

$$p_1 = p_2 = \ldots = p_i = \ldots = p_m = \frac{1}{n},$$

то величина $H(A)$ принимает наибольшее значение. Интерпретация этого свойства такова: если для данного объекта ничего не известно о вероятностях реализации угроз информационной безопасности, то риск его информационной безопасности максимален. Принятие мер информационной безопасности по любой j - й угрозе снижает вероятность ущерба по данной угрозе при соответствующем увеличении вероятности нулевого ущерба. Как следствие, величина $H(A)$ будет уменьшаться, что свидетельствует об уменьшении риска информационной безопасности.

5. Для двух объектов A и B информационная безопасность выше у того объекта, риск информационной безопасности которого ниже. Если $H(A) > H(B)$, то разность $\left[H(A) - H(B)\right]$ показывает, насколько система информационной безопасности объекта B лучше, чем информационная безопасность объекта A

Вывод: использование энтропийного подхода дает возможность построить интуитивно более корректную базу количественного сравнения систем информационной безопасности, т.к. оперирует формой распределения случайной величины, а не ее конкретными значениями.

1. *ISO/IEC Guide 73:2007.* Risk management. Vocabulary.
2. *ISO/IEC 27005:2008.* Информационная технология. Методы защиты. Менеджмент рисков информационной безопасности.
3. *ДСТУ 13335-1:2003.* Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 1. Концепції та моделі безпеки ІТ.
4. *Королев В.Ю., Бенинг В.Е., Шоргин С.Я.* Математические основы теории риска: Учебн. пособ. – М.: ФИЗМАТЛИТ, 2007. – 544 с.
5. *Лукацкий А.* Управление рисками – профанация или реальность. - Cisco Systems, Inc. - 2008. www.slideshare.net/lukatsky/ss-presentation-642004/.
6. *Руководство по управлению рисками безопасности.*// Группа разработки решений Майкрософт по безопасности и соответствию регулятивным нормам (MSSC) и центр Microsoft Security Center of Excellence (SCOE). Корпорация Майкрософт, 2006.
7. *Берколайко М., Руссман И.* Новые модели управления ресурсами банка. – «Банковское дело в Москве», № 6. – 2003. С.58-59.
8. *Прангишвили И.В.* Энтропийные и другие системные закономерности: Вопросы управления сложными системами / И.В. Прангишвили; Ин-т проблем управления им. В.А. Трапезникова. – М.: Наука, 2003. – 428 с.
9. *Волькштейн М.В.* Энтропия и информация. – М.: Наука. 1986. – 192 с.

Поступила 26.02.2009р.