УДК 681.3.06

А.В. Потий[1], Д.Ю. Пилипенко[2]

[1]*Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков*
[2]*Харьковский национальный университет радиоэлектроники, Харьков*

КЛАССИФИКАЦИЯ ПОКАЗАТЕЛЕЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В статье проводится анализ моделей показателей безопасности, а также основные таксономии показателей безопасности. В ходе анализа выделены присущие таксономиям показателей безопасности достоинства и недостатки. На основании проведенного анализа предложено направление для дальнейших исследований.

Ключевые слова: *метрика безопасности, показатель безопасности информации, таксономия показателей.*

Введение

В настоящий момент разработано множество механизмов и средств защиты информации, и теперь одной из самых приоритетных задач становится оценка эффективности процесса обеспечения информационной безопасности на основе показателей безопасности или метрик безопасности (security metrics). Классификация показателей безопасности предполагает четкое определение понятий в данной сфере. Необходимо отметить, что единодушия в трактовке понятия «метрика безопасности» не существует. Если рассматривать ситуацию в целом, то данное понятие включается целый ряд других понятий: оценка, измерение, ранжирование, рейтинги, счет и т.д. Несмотря на то, что исследователями используются, по сути, нетождественные понятия, под метриками безопасности подразумевается, как правило, вычисленная, относительная или обобщенная величина, которая предоставляет дополнительную информацию относительно наблюдаемого явления (события, объекта), имеющего отношение к защите информации. Наиболее подходящим понятием к термину метрика безопасности в русском языке яв-

ляется «показатель», поэтому в дальнейшем будем использовать данный термин.

1. Модели показателей безопасности

Для того чтобы в полной мере понять каким образом можно построить различные показатели, необходимо обратиться к уже существующим моделям показателей безопасности. Одной из первых была опубликована модель Кацке (S. Katzke) [1], в которой автор продемонстрировал взаимосвязь объектов, которые должны быть измерены (например, продукт, система, кадры, профессиональная компетенция организации в целом), целей безопасности (достижение которых оценивается) и методов оценки. Данная модель представлена на рис. 1.

Примерно в одно время с моделью Кацке была предложена другая модель показателей – модель Деборы Бодо (Deborah Bodeau) [2]. Автором было предложено рассматривать показатели безопасности как векторное произведение объекта измерения, цели измерения и лица, для которого предназначен результат измерений.

Рис. 2 иллюстрирует данную концепцию. Данная модель примечательна в первую очередь тем, что ею в определенной мере руководствовались Vaughn и др. при разработке своей таксономии показателей безопасности [3].

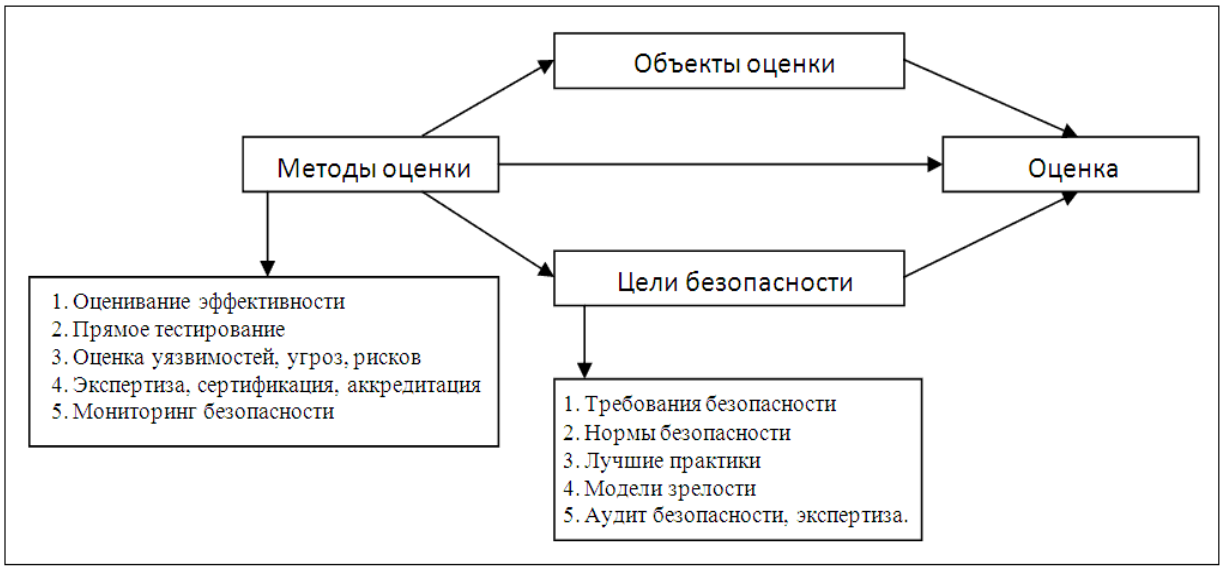

Рис. 1. Модель показателей безопасности Кацке

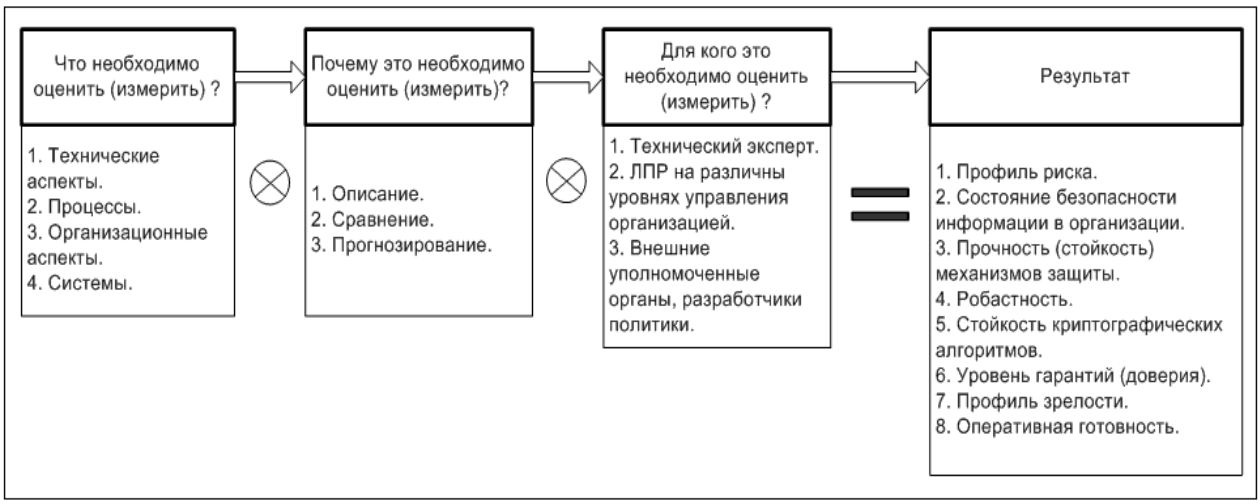

Рис. 2. Модель показателей безопасности Бодо

Несмотря на некоторые различия, авторы упомянутых моделей выражают единодушие относительно следующих моментов: необходимо четко понимать, что является объектом измерения (оценки) и с какой целью проводится измерение (оценка). Стоит отметить, что в модели Бодо также подчеркивается важность субъекта, для которого предназначается результат измерений (оценки). В своей рабо-

те Vaughn и др. высказывали опасения относительно возможной ситуации, когда недооценивается важность целей и субъекта измерения [3]. Если проводить измерения или оценку, не учитывая все перечисленные рекомендации, то существует большая вероятность, что использование показателей безопасности превратится в самоцель. Данная ситуация к тому же крайне невыгодна тем, что помимо напрасно проделанной работы, потрачены будут также ресурсы организации и время сотрудников.

2. Анализ существующих таксономий показателей безопасности

Практически одновременно с началом работ по разработке показателей безопасности и их практического применения возникла задача создания некоторой системы показателей, которая способна комплексно охарактеризовать состояние безопасности информации. Специалисты пришли к мнению, что разработка системы показателей безопасности, которая объективно отражает состояние безопасности информации на объекте информатизации, может быть выполнена в контексте таксономии, поскольку она обеспечивает логическое группирование показателей безопасности и демонстрирует взаимосвязь между этими группами. В скором времени после конференции WISSRR [2] специалисты начали предлагать свои решения относительно таксономий показателей безопасности. Первая предложенная таксономия показателей безопасности, состояла из трех категорий: организационные, операционные и технические показатели. Впрочем, детализации этих категорий предложено не было.

Самыми известными на данный момент таксономиями показателей являются следующие таксономии: Vaughn-Hennig-Siraj [3], NIST [4], OCIPEP [5], OCTAVE [6], CISWG [7], Erkan Kahraman [8]. В основе каждой из таксономий лежит некоторый принцип, по которому все множество показателей было упорядочено. Анализ данных таксономий позволил выделить следующие системы: системы, состоящие исключительно из количественных показателей (CISWG); системы, предполагающие исключительно качественную оценку (OCTAVE); смешанные системы показателей (NIST, Erkan Kahraman).

Общим и самым существенным недостатком данных таксономий является то, что ни в рамках одной из таксономий, ни в рамках всего направления не было предложено рекомендаций по получению обобщенных (комплексных) оценок. Именно такие показатели и представляют наибольший интерес, наилучшим образом способствуя принятию управленческих решений по вопросам обеспечения информационной безопасности. Необходимо отметить, что получения только количественных результатов недостаточно – основная сложность анализа информационной безопасности заключается в качественной интерпретации конкретных значений показателей.

В настоящий момент наиболее распространенной классификацией показателей является классификация по типу объекта оценки. Однако зачастую для построения эффективной системы показателей (к примеру, надежности и качества ПО как составляющей ИБ предприятия) необходимо уметь классифицировать показатели по следующим признакам:

– предмету анализа;
– процессу жизненного цикла системы (процесса);
– точности результата;
– типу шкал;
– достоверности результата.

Проанализировав существующие таксономии показателей безопасности, можно прийти к выводу, что существует несколько основных факторов, мешающих их повсеместному внедрению и применению:

– отсутствие четкой формулировки самого понятия «показатель безопасности», низкая объективность получаемой оценки;
– трудности, связанные с получением количественных результатов оценки объектов безопасности, что в свою очередь обуславливает трудности в обобщении и сравнении полученных результатов;
– отдельные трудности, связанные непосредственно с операционными показателями безопасности, проистекающие из невозможности предсказать реальное функционирование системы;
– сама природа проблем обеспечения безопасности информации.

Стоит отметить, что определенный интерес представляет задача измерения человеческого фактора в обеспечении безопасности информации. Однако здесь наблюдается противоречие между измерениями и защитой приватности. По этой же причине понятно желание не нанести ущерба личным интересам сотрудников, чья деятельность будет подлежать оценке. Здесь важными направлениями является оценка компетентности, мотивации, лояльности персонала, оценка уровня знаний и практических умений сотрудников в области обеспечения безопасности информации.

Заключение

Одним из главных желаемых свойств таксономии показателей безопасности является ее применимость в организациях различного типа и, что немаловажно, простота и понятность. Однако создание подобной таксономии сопряжено с большими труд-

ностями. Начиная с момента развития данного направления исследований и по сей день, универсальной таксономии показателей предложено не было. Более того, создается уверенность, что данное предприятие просто невозможно в силу ряда причин. Специфика и многообразие существующих организаций неизбежно означает процесс адаптации и последующей интеграции любой готовой таксономии, что в любом случае приведет к модификации исходной концепции. После интеграции система показателей должна непрерывно эволюционировать одновременно со всеми процессами организации и учитывать динамику непрерывно меняющейся внешней и внутренней среды, что снова означает уход от жесткой системы показателей. Также фиксированные таксономии плохо масштабируются, что означает возможную избыточность для некрупных организаций.

Таким образом, дальнейшее направление исследований представляется скорее в виде разработки методики построения систем показателей безопасности, чем некоторой готовой таксономии. Подобная методика позволит отойти от жестко фиксированной таксономии показателей в сторону рекомендациях к созданию гибкой эффективной системы показателей.

Список литературы

1. Katzke S. Security Metrics. Information Assurance Solutions Group, National Security / S. Katzke. – Agency, USA, 2001. – 320 p.

2. Workshop on Information, Security System Scoring and Ranking (WISSSR, 2001) Information System Security Attribute Quantification or Ordering (Commonly but improperly known as Security Metrics) – Workshop Proceedings – May 21-23, 2001, Williamsburg, VA.

3. Rayford Vaughn Jr. Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy / Vaughn Jr. Rayford, Henning Ronda, Siraj Ambareen // 30th Hawaii International Conference on System Sciences. – Big Island, Hawaii, January 7- 10, 2002. – P. 37-38.

4. NIST SP 800-55, Security Metrics Guide for Information Technology Systems, July 2008.

5. Public Safety and Emergency Preparedness Canada. National Critical Infrastructure Assurance Program Selection Criteria to Identify and Rank Critical Infrastructure Assets, January 20, 2004.

6. Alberts, Christopher J., Sandra G. Behrens, Richard D. Pethia, and William R. Wilson. September 1999. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Framework, Version 1.0. Technical Report CMU/SEI-99-TR-017.

7. Corporate Information Security Working Group (CISWG). November 17, 2004 (Revised January 10, 2005). Report of the Best Practices and Metrics Teams, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. Government Reform Committee, United States House of Representatives.

8. Erkan Kahraman. Evaluating it security performance with quantifiable metrics. Master's thesis, DSV SU/KTH, 2005.

Поступила в редколлегию 24.03.2010

Рецензент: д-р техн. наук, проф. А.С. Петров, Восточноукраинский национальный университет им. Владимира Даля, Луганск.

КЛАСИФІКАЦІЯ ПОКАЗНИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ

О.В. Потій, Д.Ю. Пилипенко

У статті проводиться аналіз моделей показників безпеки, а також основні таксономії показників безпеки. В ході аналізу виділені властиві таксономіям показників безпеки гідність і недоліки. На підставі проведеного аналізу запропоновано напрям для подальших досліджень.

Ключові слова: *метрика безпеки, показник безпеки інформації, таксономія показників*

SECURITY METRICS CLASSIFICATION

A.V. Potiy, D.J. Pilipenko

The analysis of models of indexes of safety, and also basic taxonomies of indexes of safety, is conducted in the article. During an analysis the inherent are selected taxonomies of indexes of safety of dignity and failings. On the basis of the conducted analysis direction is offered for further researches.

Keywords: *birth-certificate of safety, index of safety of information, taxonomies of indexes.*