БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin*. Breaking 104 bit WEP in less than 60 seconds [Электронный ресурс] / Режим доступа: http://eprint.iacr.org/2007/120.pdf, свободный. – Загл. с экрана.

2. Aircrack manual [Электронный ресурс] / Режим доступа: http://www.aircrack-ng.org/doku.php, свободный. – Загл. с экрана.

3. *Adam Stubble_eld, John Ioannidis, and Aviel D. Rubin.* A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). ACM Transactions on Information and System Security, 7(2):319{332, May 2004.

4. *Erik Tews.* Attacks on the wep protocol. Cryptology ePrint Archive, Report 2007/471, 2007. [Электронный ресурс] / Режим доступа: http://eprint.iacr.org/. - свободный. – Загл. с экрана.

Емельянов Константин Игоревич
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: kostaemrlyanov@gmail.com.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; аспирант.

Emelianov Konstantin Igorevich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: kostaemrlyanov@gmail.com.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
The Department of IT Security; post-graduate student.

УДК 007.51:004.822

М.И. Тенетко, О.Ю. Пескова

АНАЛИЗ И ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ С ИСПОЛЬЗОВАНИЕМ НЕЧЁТКОЙ СЕМАНТИЧЕСКОЙ СЕТИ

В данной статье предложен новый подход к описанию информационного риска, основанный на нечётких множествах и нечётких семантических сетях. Проведено теоретико-множественное исследование структуры риска. Построена нечёткая семантическая сеть, описывающая структуру риска. Сделаны выводы относительно практического применения рассмотренного подхода.

Анализ рисков; нечеткие множества; нечеткие семантические сети.

M.I. Tenetko, O.U. Peskova

ANALYSIS AND RISK ASSESSMENT INFORMATION USING FUZZY SEMANTIC WEB

In the given article a new fuzzy sets and fuzzy semantic networks based approach to description of informational risk is proposed. A set-theoretical analysis of a risk struc-

ture is realized. A fuzzy semantic network describing a risk structure is plotted. A summary concerning a practical use of the given aprroach is drawn.

Analysis of a risk structure; fuzzy sets; fuzzy semantic networks

Введение

Проект по разработке и внедрению системы управления информационной безопасностью отличается от «классических» инвестиционных проектов тем, что требует определённых инвестиций, но при этом не приносит непосредственной прибыли, не даёт прямой возможности для получения дохода. Его основная цель — обеспечение непрерывности бизнес-процесса организации, устранение возможности неполучения прибыли. Это далеко не всегда представляется очевидным для руководства организации, поэтому необходимо убедительно обосновать необходимость (и достаточность) затрат на проектирование и внедрение СУИБ. Иными словами, помимо требования научно-технической обоснованности СУИБ, изложенного в стандартах, специалист по информационной безопасности вынужден ввести требование финансовой обоснованности СУИБ, выдвигаемое экспертизой проекта.

Для обоснования необходимости инвестиций в систему информационной безопасности на начальном этапе применяются методы оценки риска и ущерба.

Существует три подхода к анализу информационных рисков. Первый подход основан на рекомендациях, отражающих наиболее успешную практику управления информационной безопасностью. Эти рекомендации изложены в специально разработанных международных и национальных стандартах. Очевидным достоинством стандартизированного подхода к анализу рисков являются сравнительно небольшие финансовые, трудовые и временные затраты на исследование.

Однако в то же время рамки стандартизации порождают ряд проблем. Во-первых, стандартизированный подход ориентирован, прежде всего, на формальную сертификацию информационной системы и СУИБ. Однако сертификация соответствия стандарту сама по себе ещё не гарантирует достижения более высокого уровня организации информационной системы и наличия работающей и эффективной СУИБ. В данном случае формальная сертификация полезна до тех пор, пока руководство организации не начинает чрезмерно доверять её результатам. Во-вторых, типовое поле рисков, отражённое в стандарте, может оказаться уже действительного поля рисков, присущего исследуемой системе. Ряд нетипичных, специфичных для данной системы рисков может выпадать из поля зрения исследования. В-третьих, элементы информационной системы, для которых рассмотрены типичные риски, как правило, рассматриваются изолированно друг от друга. На практике же любая сравнительно сложная система обладает свойствами эмерджентности и неразделимости.

Еще один подход основан на использовании математических методов, например, табличного метода, методов анализа иерархий, ожидаемых потерь. Основные недостатки можно описать кратко следующим образом:

– излишняя формальность, «сухость», ведущая к отсутствию гибкости;

– адекватность оценок ситуации действительным представлениям эксперта о ситуации;

– неспособность к эффективному анализу ситуаций, описанных без применения чисел и неструктурированных (уникальных) ситуаций.

По этой причине многие специалисты предпочитают использовать третий подход – качественный подход к анализу информационных рисков. Под качественным анализом понимается относительно неструктурированный анализ инфор-

мации разного характера, собранной экспертом при наблюдениях и беседах с сотрудниками.

Такой подход, в отличие от описанных ранее подходов, позволяет выявить не столько типовые, очевидные риски, сколько:

– неочевидные, слабоструктурированные рисковые ситуации, в которых риск возникает лишь в результате взаимосвязи большого числа неоднозначно связанных событий;

– ранее неизвестные рисковые ситуации, для выявления которых необходим системный подход с применением базовых принципов информационной безопасности.

Одним из наиболее распространённых методов выявления информационных рисков является применение опросников и анкетирование [1–3]. Эксперт (или группа экспертов) отвечает на предъявленные вопросы, затем на основании их ответов делается заключение о том, что система подвержена тем или иным рискам.

Однако практика показывает, что намного более эффективным является подход, при котором опытный специалист исследует и наблюдает оцениваемую систему, собирая предварительные данные [4]. Анализ этих данных выявляет некоторые события и состояния, которые, с точки зрения эмпирического опыта и интуиции эксперта, могут свидетельствовать о наличии риска. Что характерно, такой подход позволяет выявить не столько типовые, очевидные риски, сколько неочевидные, слабоструктурированные рисковые ситуации, в которых риск возникает лишь в результате взаимосвязи большого числа неоднозначно связанных событий.

Кроме того, можно количественно подсчитать такие составляющие ущерба, как убыток в результате простоя бизнес-процесса, затраты на восстановление корпоративной информационной системы, оплата сверхурочного труда работников, судебные издержки и некоторые другие. Однако есть составляющие, не поддающиеся подсчёту: имидж и репутация компании, нанесённый моральный ущерб. Неполучение прибыли от удара по имиджу и снижения репутации может в некоторых случаях существенно превысить затраты на создание системы информационной безопасности.

Очевидно, что на сегодняшний день не существует комплекса инструментов, который мог бы взять на себя часть функций эксперта, в частности, структурированное описание информационного риска на основе неполных, неточных и, возможно, противоречивых данных. Тем интереснее становится задача проектирования такого программного обеспечения. Рассмотрим подробнее, как можно реализовать эту функцию.

1. Нечёткие множества и нечёткие семантические сети

Для описания информационного риска на основе неточных и противоречивых данных можно использовать нечёткие множества и нечёткие семантические сети.

Напомним, что нечёткое множество – это обобщённое понятие множества, степень принадлежности которому лежит в интервале [0, 1], не ограничиваясь значениями {0, 1}. Нечёткое множество отличается от обычного множества тем, что относительно принадлежности элементов нечёткому множеству нет однозначного ответа «да» или «нет» [5].

Семантическая сеть в простейшем случае представляет собой ориентированный граф, вершины которого соответствуют объектам (понятиям, концептам) предметной области, а рёбра – связям (отношениям) между ними. Граф можно записать в виде G (V, E), где V – множество вершин, а E – множество двухместных

отношений между вершинами, называемых рёбрами. Семантическая сеть даёт возможность представлять знания о предметной области в естественной, наглядной и структурированной форме, что не всегда возможно при других способах представления знаний [6].

Связь между понятиями семантической сети выражает минимальный объём знаний, простейший факт, относящийся к двум понятиям. Более сложные утверждения в рамках семантической сети могут быть определены путём выделения соответствующих подграфов. В естественном языке такие подграфы выделяются с помощью отдельных законченных предложений, которые описывают определённые ситуации, возникающие между понятиями.

Для привнесения нечёткости в семантическую сеть, выраженную графом G (V, E), достаточно определить множество рёбер E как нечёткое множество [7]. Это даст возможность определять степень истинности утверждения, выражаемого двухместным отношением, как степень принадлежности к множеству E, лежащую в интервале [0, 1].

2. Нечёткая семантическая сеть, описывающая структуру риска

В качестве примера, иллюстрирующего применение описанных методов, приведём нечёткую семантическую сеть, описывающую структуру риска и содержащую данные для определения величины ущерба.

С нашей точки зрения, величина ущерба зависит от критичности информационного актива и подверженности тому или иному риску. В свою очередь, понятие риска включает в себя взаимодействие между угрозой и уязвимостью.

Итак, определим следующие множества: множество угроз – $\tilde{T} = \{t_1/\mu_{\tilde{T}}(t_1), t_2/\mu_{\tilde{T}}(t_2), ..., t_k/\mu_{\tilde{T}}(t_k)\}$, множество уязвимостей – $\tilde{V} = \{v_1/\mu_{\tilde{V}}(v_1), v_2/\mu_{\tilde{V}}(v_2), ..., v_m/\mu_{\tilde{V}}(v_m)\}$ и множество активов $A = \{a_1, a_2, ..., a_n\}$. Множество активов A является чётким: предприятие, безусловно, имеет чёткое представление о своих тайнах. Множества угроз T и уязвимостей V являются нечёткими: к ним допустимо относить события и ситуации, которые не могут быть однозначно классифицированы как угроза или уязвимость (это преимущественно слабоструктурированные или неизвестные ранее угрозы и уязвимости).

Нам необходимо каким-то образом обозначить критичность актива. Основная сложность заключается в том, что мы в данном случае не можем назвать чёткое множество, элементы которого могли бы количественно охарактеризовать значимость, ценность, критичность информационных активов для бизнес-процессов компании. То есть мы не знаем, как выразить степень ценности актива в форме функции тех или иных точно измеренных величин.

Шкала стоимости активов, финансовых потерь в случае нарушения безопасности активов и тому подобное не может быть использована, поскольку довольно часто нет возможности определить точную сумму стоимости либо потерь. Помимо этого, при использовании численных шкал нет возможности учесть некоторые качественные показатели такие, как снижение репутации, удар по имиджу и моральный ущерб.

В этом случае мы могли бы определить класс ценных активов и приписывать каждому активу a_s степень принадлежности к этому классу. Разумеется, полученные таким образом значения функции принадлежности основаны лишь на впечатлениях эксперта, которые он не в состоянии точно формализовать.

Другими словами, эксперт определяет функцию принадлежности не на множестве математически точно определённых объектов, а на множестве обозначенных некими символами впечатлений. Такие определения имеют смысл для человека, но не для ЭВМ, однако, тем не менее, могут обрабатываться при помощи ЭВМ.

Выделим дополнительное нечёткое множество $\tilde{C}$, характеризующее критичность актива. Множество – условно пустое; в процессе оценивания риска оно будет заполняться активами с той или иной степенью принадлежности.

Учитывая это, определим множество всех возможных сочетаний угроз и уязвимостей (множество рисков R), являющееся декартовым произведением множеств T и V и состоящее из упорядоченных пар $r = (t_k, v_m)$:

$$R = T \times V = \{(t_1, v_1), (t_1, v_2), ..., (t_k, v_m)\} = \{(t_p, v_q)\}, \quad (1)$$

где p = 1, 2, ..., k, а q = 1, 2, ..., m.

Затем определим нечёткое множество, характеризующее истинность отношения угрозы и уязвимости:

$$\tilde{R} = \{(t_1, v_1)/\mu_{\tilde{R}}(t_1, v_1), (t_1, v_2)/\mu_{\tilde{R}}(t_1, v_2), ..., (t_k, v_m)/\mu_{\tilde{R}}(t_k, v_m)\} = \\ = (t_p, v_q)/\mu_{\tilde{R}}(t_p, v_q)\}, \quad (2)$$

где p = 1, 2, ..., k, а q = 1, 2, ..., m.

Как видно, множество $\tilde{R}$ есть множество кортежей, первым компонентом которых являются элементы $t_p \in T$, вторым – элементы $v_q \in V$, а третьим – элементы $\mu_{\tilde{R}} \square \in M$. Множество R, определённое формулой (1), является универсальным множеством множества $\tilde{R}$, а множество M является множеством значений функции принадлежности из диапазона [0, 1].

Поясним смысл нечёткого множества $\tilde{R}$. Значение принадлежности упорядоченной пары из множества R к множеству $\tilde{R}$ – это субъективное выражение уверенности эксперта в том, что для исследуемой информационной системы угроза t_p реализуется через уязвимость v_q.

Далее, результатом определения ценности активов является множество $\tilde{C} = \{c_s/\mu_{\tilde{C}}(c_s)\}$ – множество упорядоченных пар, первым компонентом которых являются элементы c_s, эквивалентные некоторому $a_s \in A$, а вторым компонентом – элементы $\mu_{\tilde{C}}(c_s) \in M$. Множество активов A является универсальным множеством множества $\tilde{C}$, а множество M является множеством значений функции принадлежности из диапазона [0, 1]. Каждая упорядоченная пара устанавливает соответствие между активом a_s и значением $\mu_{\tilde{C}}(c_s)$, характеризующим степень принадлежности актива к классу критичных активов.

Наконец, чтобы сопоставить риск и актив, расширим кортеж $\{(t_p, v_q)/\mu_{\tilde{R}}(t_p, v_q)\}$, описанный в формуле (2), до вида $\{(((t_p, v_q)/\mu_{\tilde{R}}(t_p, v_q)), (c_s/\mu_{\tilde{C}}(c_s)))/\mu_{\tilde{W}}\}$. Как видно, полученный кортеж представляет собой нечёткое бинарное отношение двух других кортежей. Первый из них, в свою очередь, явля-

ется нечётким бинарным отношением между угрозой и уязвимостью. Второй является совокупностью нечёткого элемента множества критичных активов и степени его принадлежности к этому множеству. Значение $\mu_{\tilde{W}}$ являет собой характеристику истинности высказывания о том, что совокупность угрозы t_p и уязвимости v_q поражает актив $a_s \equiv c_s$, обладающий степенью ценности $\mu_{\tilde{C}}(c_s)$. Совокупность таких кортежей составляет множество $\tilde{W}$.

Такое представление учитывает одновременно ценность актива и степень связанности угрозы с уязвимостью, что даёт возможность впоследствии оценить величину риска нарушения безопасности данного актива.

Итак, мы описали нечёткие отношения между угрозами, уязвимостями, рисками, активами и классом критичных активов. Нечёткий ориентированный граф, соответствующий этим отношениям и выражающий нечёткую семантическую сеть понятия «ущерб», представлен на рис. 1.

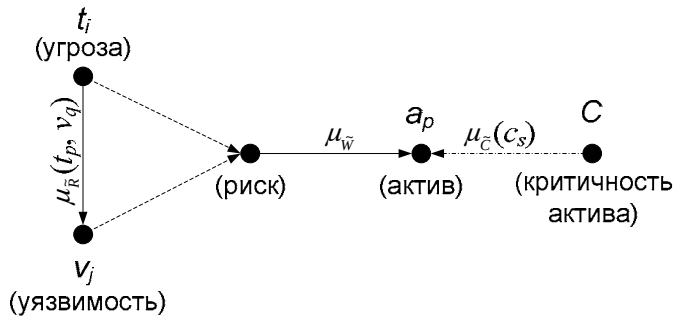

Рис. 1. Семантическая сеть, соответствующая понятию «ущерб»

Обратим внимание, что в данной семантической сети отражены три вида связей. Сплошными линиями показаны связи влияния (воздействия) одного понятия на другое, пунктиром показаны генеративные связи (объединяющие несколько простых понятий в сложное понятие), пунктиром с точками показаны связи между свойством понятия и понятием.

Заключение

Мы подробно рассмотрели один из методов формализации и обработки неточных и противоречивых данных. Применение этого метода может лечь в основу программной системы поддержки принятия решений, которая выполняет часть функций эксперта в области информационной безопасности.

Предполагается максимально упростить ввод данных в систему: свести его к выбору типовых блоков семантической сети и представлению нечётких значений в виде визуального образа (например, в виде градиента цвета или прозрачности).

Нечёткие данные, полученные в результате описания риска, могут стать входом нечёткой продукционной модели с базой знаний, выраженных в виде нечётких правил. Выходом продукционной модели будет являться решение о величине возможного ущерба.

Возможно также исследовать подходы к созданию базы знаний, которая позволила бы давать рекомендации относительно того, какие меры наиболее целесо-

образны для борьбы с каждым отдельным риском. Однако эта задача является достаточно сложной, и её решение может потребовать участия большой группы специалистов в разных областях науки и техники.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Insight Consulting Home Page. – http://www.insight.co.uk/

2. RiskWatch Home Page. – http://www.riskwatch.com/

3. Digital Security Office Home Page. – http://www.dsec.ru/products/dsoffice/

4. *Douglas J. Landoll* The Security Risk Assessment Handbook. A Complete Guide for Performing Security Risk Assessments. – New York. : Auerbach Publications, 2006. – 504 p.

5. *Круглов В.В.* Нечёткая логика и искусственные нейронные сети. / В.В. Круглов, М.И. Дли, Р.Ю. Голунов. – М. : Физматлит, 2001. – 224 с.

6. *H. Helbig* Knowledge Representation and the Semantics of Natural Language. – Berlin. : Springer-Verlag, 2006. – 647 p.

7. *Берштейн Л.С.* Нечёткие графы и гиперграфы. / Л. С. Берштейн, А. В. Боженюк. – М. : Научный мир, 2005. – 255 с.

Тенетко Михаил Иванович
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: tenetko@gmail.com.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; аспирант.

Tenetko Mihail Ivanovich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: tenetko@gmail.com.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
The Department of IT Security; post-graduate student.

Пескова Ольга Юрьевна
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: poy@tsure.ru.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; доцент.

Peskova Olga Urevna
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: poy@tsure.ru.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
The Department of IT Security; associate professor.