8. *Кащенко А.Г.* Задача многокритериального синтеза структуры и параметров системы защиты информации // Информация и безопасность: региональный научно-технический журнал. – Воронеж, 2006. – Вып. 2. – С. 107 – 110.

9. *Машкина И.В., Гузаиров М.Б.* Интеллектуальная поддержка принятия решений по управлению защитой информации в критически важных сегментах информационных систем // Приложение к журналу «Информационные технологии». – 2008. – №7. – 2 с.

Михеев Вячеслав Алексеевич
Открытое акционерное общество «Концерн радиостроения “Вега”».
E-mail: mikheev@vega.su.
121170, г. Москва, Кутузовский проспект, 34.
Тел.: 8 (499) 2490585.
Заместитель директора.

Mikheev Viatcheslav Alekseevich
Joint-Stock Company «Radio Engineering Corporation “VEGA”».
E-mail: mikheev@vega.su.
34, Kutuzov avenue, Moscow, 121170, Russia.
Phone: 8 (499) 2490585.
The deputy director.

УДК 004.942 - 004.827

Г.А. Евстафьев

НЕЧЁТКИЕ КОГНИТИВНЫЕ КАРТЫ ПРИМЕНИТЕЛЬНО К УПРАВЛЕНИЮ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Предлагается подход для управления рисками информационной безопасности на основе нечётких когнитивных карт и искусственных нейронных сетей. В подходе предлагается разделить понятия риска на две составляющие: системозависимый и системонезависимый риски. Данный подход позволяет уменьшить долю субъективизма при оценке риска информационной безопасности (ИБ) организации, учесть все элементы, участвующие и не участвующие в обработке данных в АС, и автоматизировать процесс управления рисками.

Управление рисками ИБ; нечёткие когнитивные карты; актив; сканеры безопасности.

G.A. Evstafiev

FUZZY COGNITIVE MAPS IN RELATION TO RISK MANAGEMENT INFORMATION SECURITY

The paper proposes an approach to risk management of information security based on fuzzy cognitive maps and artificial neural networks. In the approach proposed to divide the notion of risk into two components: a system-dependent and system-independent risks. This approach allows to reduce the proportion of subjectivity in assessing the risk of information security organization, consider all the elements involved and not involved in the processing of data in the Automatic Systems and automate the process of risk management.

Risk Management information security; fuzzy cognitive maps; asset; security scanners.

Как считалось издревле: кто владеет информацией, тот владеет ситуацией и контролирует её. В свете развития информационных технологий, потребность в защите информации возрастает с каждым днём всё больше. Но работа, передача и защита информации связана с риском, который необходимо учитывать и оценивать, а также им необходимо управлять для успешной работы организации.

Известно, что риск – это вероятность реализации угрозы информационной безопасности. В классическом представлении оценка рисков включает в себя оценку угроз, уязвимостей и ущерба, наносимого при их реализации. Анализ риска заключается в моделировании картины наступления этих самых неблагоприятных условий посредством учета всех возможных факторов, определяющих риск как таковой. С математической точки зрения при анализе рисков такие факторы можно считать входными параметрами.

Проблема возникает тогда, когда в оценку риска информационной безопасности вовлекается человек, которые привносит в нее степень субъективности. Также при использовании табличных методик оценки и управления рисками информационной безопасности, которые в большей степени используются в данный момент на рынке, вводится доля субъективизма, и данные методики зачастую не автоматизированы.

1. Краткий обзор стандартов управления рисками ИБ

В мировой практике уже сравнительно давно осуществляется процесс управления рисками ИБ. Этот процесс регламентируется рядом международных стандартов, таких как британский стандарт BS 7799-3:2006, международный стандарт BS ISO/IEC 27001:2005.

Стандарт BS 7799-3:2006 предлагает процессный подход к оценке рисков, их обработке, непрерывному мониторингу, пересмотрам и переоценке рисков. Данный подход подчеркивает важность:

1) понимания требований ИБ бизнеса и необходимости установления политики и целей ИБ;

2) выбора, внедрения и эксплуатации механизмов контроля в контексте управления общими бизнес-рисками организации;

3) мониторинга и анализа производительности и эффективности системы управления информационной безопасности (СУИБ) для управления бизнес-рисками;

4) непрерывного совершенствования на базе объективных измерений рисков.

Данный подход представлен на рис. 1.

В стандарте описаны следующие действия и мероприятия:

1) идентификация ресурсов;

2) идентификация требований законодательства и бизнеса, применимых к идентифицированным ресурсам;

3) оценка идентифицированных ресурсов с учётом идентифицированных требований законодательства и бизнеса, а также последствий нарушения конфиденциальности, целостности и доступности;

4) оценка вероятности возникновения угроз уязвимости;

5) вычисление рисков;

6) оценка рисков по заранее определенной школе риска.

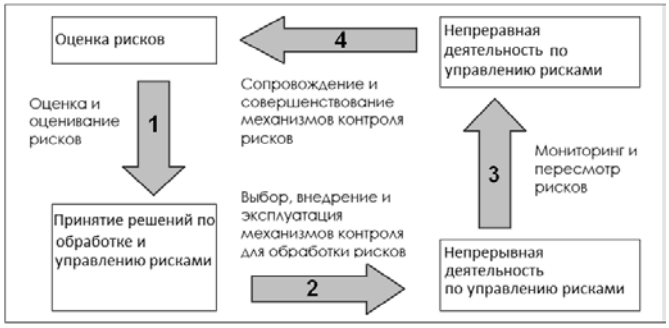

Рис. 1. Модель процессов управления рисками

Следующим шагом в процессе управления рисками является идентификация подходящих мер по обработке рисков для каждого из рисков, идентифицированных в ходе оценки рисков. Управлять рисками можно путём комбинирования превентивных и детектирующих механизмов контроля, тактики избегания, страхования и/или простого принятия риска. После того, как риск был оценен, должно быть принято бизнес решение насчет принятия необходимых мер.

После принятие решений по обработке рисков и внедрения выбранных механизмов контроля, должны начинаться непрерывные действия по управлению рисками. Эти действия включают в себя процесс мониторинга рисков и производительности СУИБ, позволяющий гарантировать, что внедренные механизмы контроля функционируют надлежащим образом. Другими действиями являются пересмотр и переоценка рисков, необходимые для адаптации оценки рисков к изменениям, которые могут со временем происходить в деловой среде [1].

Также был разработан ГОСТ Р ИСО/МЭК ТО 13335-3-2007 – Национальный стандарт Российской Федерации, методы и средства обеспечения безопасности, (Часть 3), методы менеджмента безопасности информационных технологий. Данный ГОСТ призван дать необходимые описания и рекомендации по способам эффективного управления безопасностью информационных технологий. Эти способы могут быть использованы для оценки требований по безопасности и рисков. Кроме того, они должны помочь устанавливать и поддерживать необходимые средства обеспечения безопасности, то есть правильный уровень обеспечения безопасности информационных технологий. Может возникнуть необходимость в том, чтобы результаты, полученные таким образом, были усилены за счет применения дополнительных средств защиты применительно к данной организации и данной среде. Данный стандарт предназначен для сотрудников организации, ответственных за управление безопасностью информационных технологий и/или внедрение мер обеспечения их безопасности.

2. Применение нечётких когнитивных карт и искусственных нейронных сетей для процесса управления рисками ИБ

Для решения проблемы управления рисками информационной безопасности предлагается:

1. Использовать математический аппарат нечёткой логики, в частности нечёткие когнитивные карты (НКК). Их неоспоримым достоинством по сравнению с другими методами являются возможность формализации численно неизмеримых

факторов, использования неполной, нечёткой и даже противоречивой информации [2]. А также искусственные нейронные сети для более быстрой и точной классификации актива по уровню риска.

Для построения НКК объект исследования представляют в виде знакового ориентированного графа. Пример графа представлен на рис. 2.

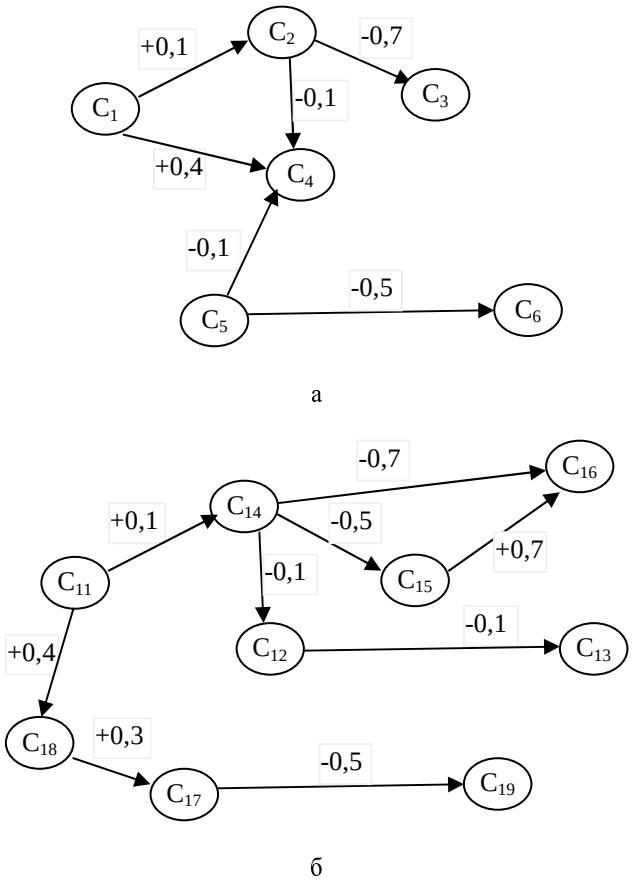

Рис. 2. Знакового-ориентированный граф: а – граф верхнего уровня, б – граф нижнего уровня

В низкоуровневом графе представлено влияние взаимосвязанных узлов в локально вычислительной сети (ЛВС) отдела, учитывая присутствующие уязвимости в программном обеспечении (ПО) на хостах. Следовательно, возможно получить предполагаемые сценарии атаки. На основе данной информации возможно построить карту верхнего уровня, которая показывает влияние отдела на отдел, учитывая все присутствующие уязвимости. Таким образом, возможно оценить риск организации.

Ключевые факторы объекта исследования располагаются в вершинах графа и называются концептами. Дуги графа отображают причинно-следственные связи между вершинами. Таким образом, НКК представляет собой картеж:

$$\text{ÍÍÊ} = \{C_n, L_{ij}, S_{g_{ij}}, W_{ij}\}, \quad (1)$$

где { C_n } – множество вершин (концептов);

{ L_{ij} } – множество причинно-следственных связей между концептами;

{ Sg_{ij} } – множество знаков связей (+,–);

{ W_{ij} } – множество весов связей (сильно, слабо, средне и т.д.).

В свою очередь, множество концептов представляет собою следующие подмножества:

$$\{C_n\} = \{C_K^G, C_i^U, C_j^M, C_l^B\}, \quad (2)$$

где { C_k^G } – подмножество целевых факторов, состояние которых является критически важным для собственника информационной системы, т.е. элементы актива;

{ C_i^U } – подмножество дестабилизирующих факторов или угроз информационной безопасности;

{ C_j^M } – подмножество управляющих факторов, с помощью которых решается задача управления рисками;

{ C_l^B } – подмножество базовых факторов, к которым относятся все остальные промежуточные концепты.

Определение концептов, их переменных состояний и связей между ними является задачей, требующей высокой квалификации эксперта, осуществляющего построение и анализ НКК.

В теории НКК вводится понятие непрямых и полных причинных эффектов [2]. Некоторый путь от концепта C_i к концепту C_j, например C_i –> C_{k1} –> … –> C_{kn} –> C_j , считается непрямым эффектом. При этом если веса причинно-следственных связей заданы, можно вычислить значение непрямого эффекта. В простейшем случае оно равно

$$T(C_i \to C_{k1} \to \ldots \to C_{kn} \to C_j) = \min\{W_{i,k1} \to W_{k1,k2} \to \ldots \to W_{kn,j}\}, \quad (3)$$

где W_{ij} – веса причинно-следственных связей между концептами (без учета знака).

При наличии нескольких различных непрямых эффектов (путей из C_i в C_j), общий полный эффект вычисляется как

$$S(C_i \to C_j) = \max\{T_1 \to T_2 \to \ldots \to T_N\}, \quad (4)$$

где T_k – непрямой эффект между C_i и C_j, N – число непрямых эффектов.

Если использовать формулу (4) для прослеживания пути от *i*-й угрозы к *j*-му элементу актива, то получится значение полного эффекта влияния угрозы на ресурс (C_i^U –> C_j^G). Таким образом, можно проследить все возможные пути влияния угроз на активы и выявить наиболее опасные.

В зависимости от характера управляющих воздействий, можно выделить несколько стратегий управления рисками [3]:

– уменьшение риска:

$$\left\{\mathrm{C_n}, L_{ij}, S_{g_{ij}}, W_{ij}\right\} => \left\{\mathrm{C_m}, L_{ij}, S_{g_{ij}}, d_{ij}, W_{ij}^{d}\right\}, \quad (5)$$

где $\{d_{ij}\}$ – множество барьеров;

– уклонение от риска

$$\left\{\mathrm{C}_n^1, L_{ij}^1, S_{g_{ij}}^1, W_{ij}^1\right\} => \left\{\mathrm{C}_\mathrm{m}^2, L_{ij}^2, S_{g_{ij}}^2, d_{ij}^2, W_{ij}^2\right\}; \quad (6)$$

– изменение характера риска

$$\left\{\mathrm{C}_j^\mathrm{M}\right\} \to \left\{\mathrm{C}_\mathrm{i}^\mathrm{B}\right\}; \quad (7)$$

– принятие риска

$$\left\{\mathrm{C}_j^\mathrm{M}\right\} => \left\{\mathrm{C}_\mathrm{i}^\mathrm{U}\right\}. \quad (8)$$

2. Разделить риск на две составляющие:

– системонезависимый риск – оценка риска производится без учёта ценности информации, которую несёт в себе оцениваемый актив. Данное значение риска вычисляется по формуле

$$r = \sum_{i=1}^{N}\sum_{j=1}^{n}\left(V_j * C_j\right)_i, \quad (9)$$

где V_i – наличие уязвимости;

C_i – степень критичности уязвимости;

N – число активов;

n – число уязвимостей;

i – индекс актива;

j – индекс уязвимости.

После этого возможно рассчитать общий риск инфраструктуры организации

$$R = \sum_{i=1}^{K} r_i, \quad (10)$$

где K – число отделов,

i – индекс отдела;

– системозависимый риск – оценка риска производится с учётом ценности информации, которая находится на активе и им используется. Данное значение вычисляется на основе НКК.

Данное значение риска вычисляется по формуле

$$r_i = \mathrm{S}\left(\mathrm{C}_\mathrm{i}^\mathrm{U} \to C_j^G\right) * A_j, \quad (11)$$

где { C_i^U } – подмножество дестабилизирующих факторов или угроз информационной безопасности,

{ C_k^G } – подмножество целевых факторов, состояние которых является критически важным для собственника информационной системы, т.е. элементы актива,

A_j – ценность элемента актива.

Данное разделение вводится для того, чтобы учесть тот фактор, что даже активы, не несущие в себе ценную информацию, могут быть использованы для получения доступа, искажения или модифицирования информации или других действий злоумышленника.

Следующим этапом управления рисками ИБ является обработка собранной информации искусственной нейронной сетью. С её помощью возможно классифицировать элементы актива по уровню риска с учётом ценности и значимости данного элемента для организации. На выходе искусственной нейронной сети будет получен конечный уровень риска данного элемента.

На рис. 3 представлен алгоритм оценки рисков ИБ.

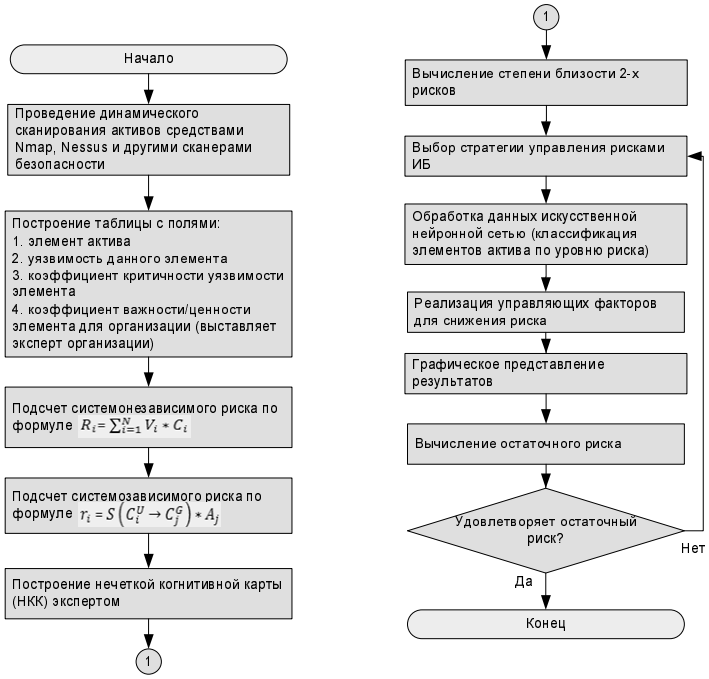

Рис. 3. Алгоритм оценки рисков ИБ

Заключение

Проблема анализа информационных рисков значительно упрощается и формализуется при использовании нечеткого когнитивного подхода в сочетании с использованием искусственных нейронных сетей. Достоинством предложенного подхода к анализу рисков на базе НКК является возможность построения адекватной модели воздействия угроз на защищаемые ресурсы и оценки их последствий при наличии неполной или даже противоречивой исходной информации. Величина предсказанных рисков и характер изменения состояния целевых факторов позво-

ляют при этом выбрать стратегию управления рисками и подобрать адекватные меры защиты для противодействия информационным угрозам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Системы управления информационной безопасностью. Ч. 3: Руководство по управлению рисками информационной безопасности BS 7799-3:2006. – С. 70.

2. *Kosko, B* Fuzzy Cognitive Maps / B. Kosko // Int. J. of Man-Machine Studies. – 1986. – Vol. 1. – P. 65 – 75.

3. *Хрусталёв Е.* Когнитивные технологии в теории и практике стратегического управления (на примере оборонно-промышленного комплекса) / Е. Хрусталёв, Д. Макаренко // Проблемы теории и практики управления. – М.: Общество с ограниченной ответственностью «Международная Медиагруппа», 2007. – С. 25–33.

Евстафьев Георгий Александрович
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: georg@evstafiev.name.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; аспирант.

Evstafiev George Aleksandrovich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: georg@evstafiev.name.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
The Department of IT Security; post-graduate student.

УДК 004.056.52

О.М. Лепешкин, П.В. Харечкин

ФУНКЦИОНАЛЬНО-РОЛЕВАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ В СОЦИОТЕХНИЧЕСКИХ СИСТЕМАХ

Представлена функционально-ролевая модель управления доступом, реализующая динамическое назначение полномочий. Модель учитывает понятие задачи, для каждой задачи определяются роли и полномочия. Представлено формальное описание модели и пример ее реализации.

Модель разграничения доступа; активное управление доступом; роль; социотехническая система; функциональная безопасность.

O.M. Lepeshkin, P.V. Kharechkin

FUNCTIONAL-ROLE-BASED ACCESS CONTROL MODEL IN SOCIOTECHNICAL SYSTEMS

The paper gives the functional-role based access control model that realizes permission dynamic management. Task is core in this model, task associates role and per-