VII Висновки

Таким чином, аналіз криптографічної стійкості механізмів блокових матричних перетворень дає можливість стверджувати, що способи криптоаналізу шляхом "статистичного" аналізу з використанням фрагментів відкритого та зашифрованого тексту, спроби обрахування прямих чи зворотних матриць, при дотриманні викладених у відповідних розділах рекомендацій, є не результативними, а кількість варіантів ключових наборів є не меншою ніж для інших відомих механізмів формування контрольних ознак.

Література: ***1.*** *Алфьоров А. П., Зубов А Ю., Кузьмін А. С., Черьомушкін А.В. Основи криптографії: Навчальний посібник. 3-тє вид., Випр. і доп. - М.: 2005. - 480с.* ***2.*** *Введення в криптографію / За заг. ред. В. В. Ященко. - 3-е вид., Доп. - М.: 2000.-288с.* ***3.*** *Нечаєв В. І. Елементи криптографії (Основи теорії захисту інформації): Учеб. Посібник для ун-тів і пед. вузів. / За ред. В. А. Садовнича - М.: Вищ. шк., 1999 - 109с.* ***4.*** *Василенко В. С. Варіант завадостійкого криптографічного перетворення // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні, вип. 8, 2004 р. –с. 101 – 108.* ***5.*** *Василенко В. С. Блокові криптографічні перетворення з використанням лишкових класів // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні, вип. 8, 2004 р. – с. 101 – 108.*

УДК 004. 516. 1

УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ НЕЧЁТКИХ КОГНИТИВНЫХ КАРТ

Богдан Волобуев, Владислав Черныш
Харьковский национальный университет радиоэлектроники

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

Summary: **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 System and automate the process of risk management.**

Ключевые слова: **Нечёткие когнитивные карты, актив, управление рисками ИБ, сканеры безопасности.**

Введение

В свете развития информационных технологий потребность в защите информации возрастает с каждым днём. Но обработка, передача и защита информации связаны с риском, который необходимо учитывать, оценивать и управлять для успешной работы организации.

В настоящее время на практике используются различные методы оценки и управления информационными рисками. Процедуры оценивания информационных рисков компании разделяют на следующие этапы :

- идентификация и количественная оценка информационных ресурсов компании, значимых для бизнеса;
- оценивание возможных угроз;
- оценивание существующих уязвимостей;
- оценивание эффективности средств обеспечения информационной безопасности.

Риск – это вероятность реализации угрозы информационной безопасности (ИБ). 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.

Возможность реализации угрозы оценивается вероятностью ее реализации в течение заданного интервала времени для некоторого ресурса компании. При этом вероятность того, что угроза реализуется, определяется следующим основными показателями:

- привлекательностью ресурса;
- возможностью использования ресурса для получения дохода;
- техническими возможностями реализации угрозы;
- степенью легкости, с которой уязвимость может быть использована.

Проблема возникает в том случае, когда в оценку риска ИБ вовлекается человек, который привносит в нее степень субъективности.

В современном мире понятие риска широко употребляется в разных сферах деятельности. Управление рисками ИБ представляет собой достаточно широкое понятие, которое используется в литературе как вид деятельности, включающий определение угроз безопасности информационной системы (ИС), оценку уровня опасности угроз (т. е. размера возможного ущерба), а также вероятностей реализации этих угроз (т. е. проведение полного анализа рисков системы). На основе анализа угроз принимается решение о мерах по снижению общего уровня риска для ИС. Причем конкретное содержание этого понятия зависит от решаемой задачи.

В соответствии с международными стандартами управления рисками ИБ компании предполагает следующее:

- определение основных целей и задач защиты информационных активов компании;
- создание эффективной системы оценки и управления рисками ИБ;
- расчет совокупности детализированных не только качественных, но и количественных оценок рисков;
- применение специального инструментария оценки и управления рисками.

Использование нечётких когнитивных карт для процесса управления рисками ИБ

Для решения проблемы управления рисками ИБ предлагается:

1. Использовать математический аппарат нечёткой логики, в частности нечеткие когнитивные карты (НКК). НКК были предложены Б. Коско в 1986 г. и используются для моделирования причинных взаимосвязей, выявленных между концептами некоторой области [2]. В отличие от простых когнитивных карт, нечеткие когнитивные карты представляют собой нечеткий ориентированный граф, узлы которого являются нечеткими множествами. Направленные ребра графа не только отражают причинно-следственные связи между концептами, но и определяют степень влияния (вес) связываемых концептов. Активное использование нечетких когнитивных карт в качестве средства моделирования систем обусловлено возможностью наглядного представления анализируемой системы и легкостью интерпретации причинно-следственных связей между концептами. Основные проблемы связаны с процессом построения когнитивной карты, который не поддается формализации. Кроме того, необходимо доказать, что построенная когнитивная карта адекватна реальной моделируемой системе. Для решения данных проблем разработаны алгоритмы автоматического построения когнитивных карт на основе выборки данных.

Их достоинством является использование искусственных нейронных сетей для более быстрой и точной классификации актива по уровню риска, а также возможность формализации численно неизмеримых факторов, использование нечёткой, неполной и противоречивой информации [2].

Для построения НКК объект исследования представляют в виде знакового – ориентированного графа. Пример графа представлен на рис. 1, 2.

В низкоуровневом графе представлено влияние взаимосвязанных узлов в локально вычислительной сети (ЛВС) отдела, учитывая присутствующие уязвимости в программном обеспечении (ПО) на хостах. Далее, возможно получение предполагаемых сценариев атаки. На основе данной информации возможно построение карты верхнего уровня, которая показывает влияние отдела на отдел, учитывая все присутствующие уязвимости. Таким образом, возможна оценка риска организации.

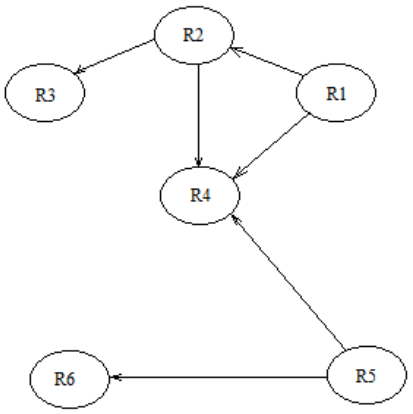

Рисунок 1 – Знаково-ориентированный граф верхнего уровня

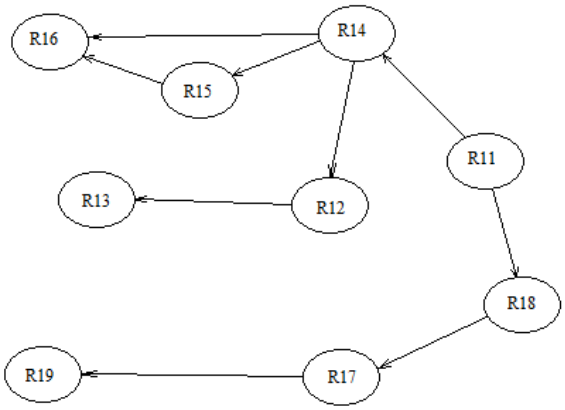

Рисунок 2 – Знаково-ориентированный граф нижнего уровня

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

$$НКК = \{R_n, F_{yg}, J_{cyg}, W_{yg}\}, \quad (1)$$

где {Rn} – множество вершин (концептов);

{Fyg} – множество причинно-следственных связей между концептами;

{Jcyg} – множество знаков связей (+,-);

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

В свою очередь, множество концептов представляет собою следующие подмножества:

$$\{R_n\} = \{R_G^K, R_b^T, R_n^U, R_v^B\}, \quad (2)$$

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

$\{R_b^T\}$ – подмножество дестабилизирующих факторов или угроз ИБ;

$\{R_n^U\}$ – подмножество управляющих факторов, с помощью которых решается задача управления рисками;

$\{R_v^B\}$ – 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 R_y к концепту R_g, например $R_y \to R_{g1} \to \ldots \to R_{gn} \to R_g$, считается непрямым эффектом. При этом если веса причинно-следственных связей заданы, можно вычислить значение непрямого эффекта.

В простейшем случае значение равно:

$$N(R_y \to R_{g1} \to ... \to R_{gn} \to R_g) = \min\{W_{y,g1} \to W_{g1,g2} \to ... \to W_{gn,g}\}, \quad (3)$$

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

При наличии нескольких различных непрямых эффектов (путей из R_y в R_g) общий полный эффект вычисляется как:

$$E(R_y \to R_g) = \max\{T_1 \to T_2 \to ... \to T_N\}, \quad (4)$$

где T_m – непрямой эффект между R_y и R_g, N – число непрямых эффектов.

Если использовать формулу (4) для прослеживания пути от y – й угрозы к j – му элементу актива, то получится значение полного эффекта влияния угрозы на ресурс $(R_y^T \to R_g^K)$. Таким образом, можно проследить все возможные пути влияния угроз на активы и выявить наиболее опасные.

В зависимости от характера управляющих воздействий выделяется ряд стратегий управления рисками [3]:

- уменьшение риска:

$$\{R_n, F_{yg}, J_{cyg}, W_{yg}\} \Rightarrow \{R_m, F_{yg}, J_{cyg}, f_{yg}, W_{yg}^f\}, \quad (5)$$

где $\{f_{yg}\}$ – множество барьеров;

- принятие риска:

$$\{R_n^U\} \Rightarrow \{R_b^T\}; \quad (6)$$

-изменение характера риска:

$$\{R_n^U\} \to \{R_v^B\}; \quad (7)$$

- уклонение от риска:

$$\{R_n^1, F_{yg}^1, J_{cyg}^1, W_{yg}^1\} \Rightarrow \{R_m^2, F_{yg}^2, J_{cyg}^2, f_{yg}^2, W_{yg}^2\}. \quad (8)$$

2. Разделить риск на две составляющие:

- системонезависимый риск – оценка риска производится без учёта ценности информации, которую несет в себе оцениваемый актив. Значение системонезависимого риска вычисляется по формуле:

$$R' = \sum_{y=1}^{N} \sum_{g=1}^{n} (D_g * R_g)_y, \quad (9)$$

где D_y - наличие уязвимости;

R_y - степень критичности уязвимости;

n – число уязвимостей;

y – индекс актива;

N – число активов;

g – индекс уязвимости.

После этого можно рассчитать общий риск инфраструктуры организации:

$$R'' = \sum_{y=1}^{K} r_y, \quad (10)$$

где K – число отделов;

y – индекс отдела.

- системозависимый риск (r_y) - оценка риска производится с учётом ценности информации, которая находится на активе и им используется. Данное значение вычисляется на основе НКК по формуле:

$$r_y = S(R_b^T \to R_g^K) * A_g, \quad (11)$$

где $\{R_b^T\}$ – подмножество дестабилизирующих факторов или угроз ИБ;

$\{R_g^K\}$ – подмножество целевых факторов, состояние которых является критически важным для собственника информационной системы;

A_g – 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 модификации информации или других действий злоумышленника.

Следующим этапом управления рисками ИБ является обработка собранной информации исскуственной 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.

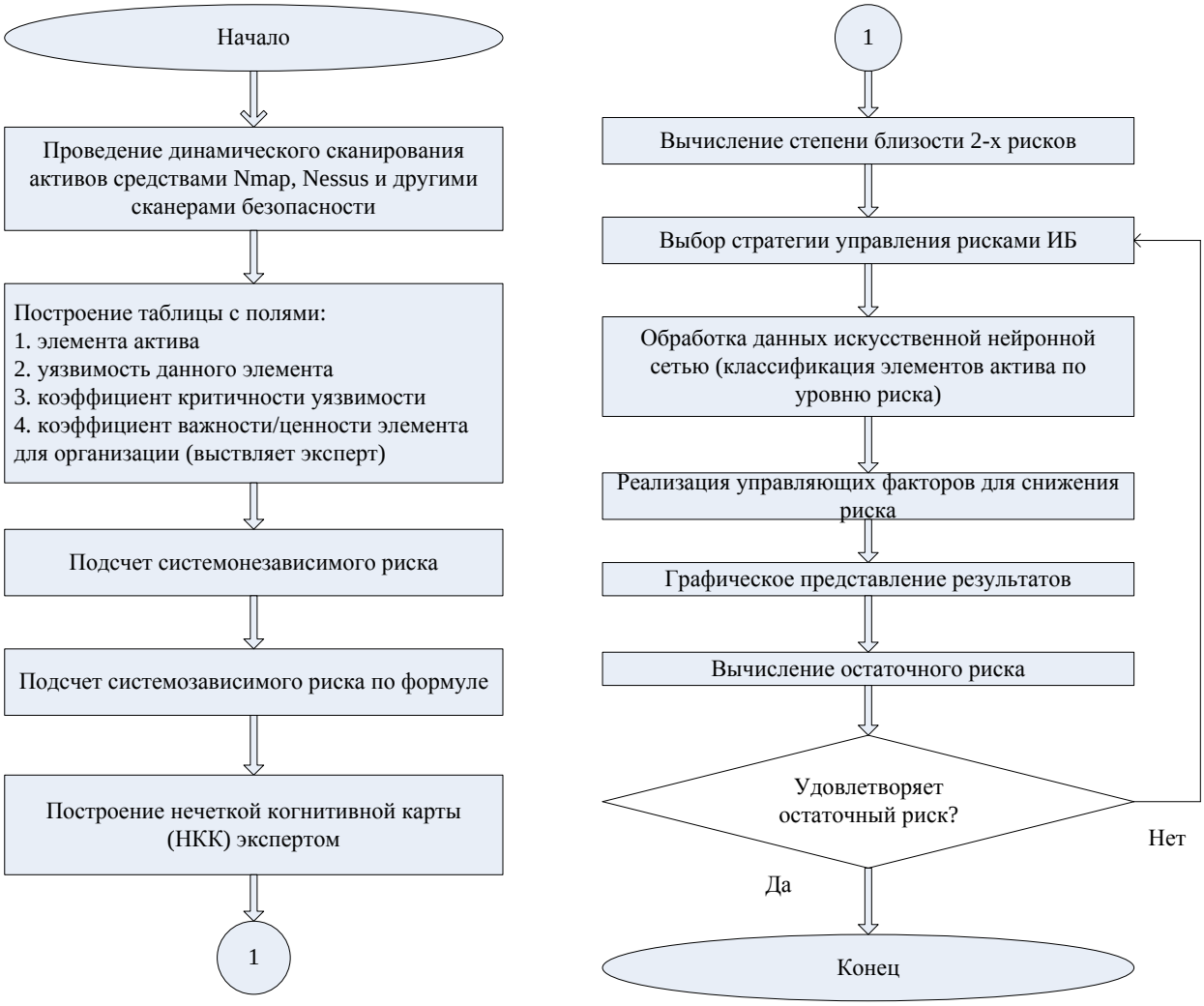

Рисунок 3 – Алгоритм оценки рисков ИБ

Выводы

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

Література: ***1.*** *Системы управления информационной безопасностью. Ч. 3: Руководство по управлению*

рисками информационной безопасности BS 7799-3:2006. – С. 70. ***2.*** *Koshko, B Fuzzy Congnitive Maps / B. Koshko // 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), 2007. – С. 25–33.*

УДК 681.3.06

ЗАЩИТА ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ОПЕРАЦИОННЫХ СИСТЕМ MS WINDOWS

Андрей Тимошенко
ООО "Институт компьютерных технологий"

Анотація: **Розглянуто проблеми забезпечення захисту інформації з обмеженим доступом в інформаційних системах на базі локальних обчислювальних мереж, побудованих із використанням комп'ютерів під керуванням операційних систем сімейства MS Windows.**
Summary: **The problems of critical information security in computer systems, based on the local area networks and computers with MS Windows operating systems are discussed.**
Ключові слова: **Інформаційна система, захист інформації.**

В настоящее время трудно представить себе предприятие или организацию, в которой не используются автоматизированные (информационные) системы, реализующие различные технологии обработки информации. В качестве основы вычислительной системы таких информационных систем (ИС), как правило, выступают локальные вычислительные сети (ЛВС) – совокупность взаимодействующих в процессе своего функционирования компьютеров, имеющих совместно используемые (разделяемые) ресурсы (жесткие диски, устройства печати и т. п.). Современные ЛВС обычно подразделяют на одноранговые – такие, в которых совместно использоваться (разделяться) могут ресурсы любого компьютера, который, таким образом, может выполнять роль как клиентской рабочей станции, так и роль невыделенного сервера, а также ЛВС с выделенными серверами – такие, в которых совместно используются ресурсы только специально выделенных компьютеров (серверов). При этом подавляющее большинство современных ЛВС, как одноранговых, так и с выделенными серверами, строятся с использованием компьютеров (рабочих станций, невыделенных и выделенных серверов), функционирующих под управлением операционных систем (ОС) семейства MS Windows. На сегодняшний день в качестве ОС рабочих станций, как правило используется MS Windows XP или MS Windows 7, а в качестве ОС серверов – MS Windows Server 2003 или MS Windows Server 2008.

Согласно НД ТЗИ 2.5-004-99 [1], ИС, о которых идет речь, могут быть классифицированы: как автоматизированные системы (АС) класса 2 – в случае, если вычислительная система ИС имеет территориально локализованный характер и построена на основе одной ЛВС; как АС класса 3 – в случае, если вычислительная система ИС имеет территориально распределенный характер и построена на основе нескольких территориально локализованных ЛВС, взаимодействие между которыми организовано с использованием каналов распределенных сетей передачи данных, например, ведомственных сетей или сети Интернет.

Целью данной статьи является анализ особенностей обеспечения защиты информации с ограниченным доступом (ИсОД), обрабатываемой в ИС, классифицируемых как АС класса 2, либо в отдельных составляющих ИС, классифицируемых как АС класса 3, при условии, что в качестве основы вычислительной системы этих ИС выступают ЛВС, построенные с использованием компьютеров, функционирующих под управлением ОС семейства MS Windows (далее – ИС на базе ЛВС). Вопросы, касающиеся защиты данных, передаваемых по каналам распределенных сетей передачи данных, не рассматриваются.

Любая информационная (автоматизированная) система [2] представляет собой организационно-техническую систему, объединяющую вычислительную систему, физическую среду, в которой функционируют компоненты вычислительной системы ИС, персонал и обрабатываемую информацию. При этом, кроме характеристик обрабатываемой информации и физической среды, одной из ключевых характеристик ИС, непосредственно влияющих на функциональный и структурный состав реализуемого комплекса средств защиты (КСЗ) информации, является архитектура вычислительной системы ИС, в