Управление рисками и безопасностью

Сравнительный анализ алгоритмов когнитивного моделирования при оценке рисков информационной безопасности*

М.Б. Гузаиров[I], А.М. Вульфин[I], В.М. Картак[I], А.Д. Кириллова[I], К.В. Миронов[I]

[I] Уфимский государственный авиационный технический университет, г. Уфа, Россия

Аннотация. В статье рассматривается применение подходов к оценке рисков информационной безопасности компьютерной сети на основе технологий интеллектуального анализа данных и когнитивного моделирования. Проанализированы основные этапы реализации оценки рисков информационной безопасности с использованием сети Байеса на основе графа атак, нечетких когнитивных карт и нечетких серых когнитивных карт, сформулированы рекомендации по их использованию.

Ключевые слова: *информационная безопасность, оценка рисков, сеть Байеса, нечеткие когнитивные карты, нечеткие серые когнитивные карты.*

DOI: 10.14357/20790279190408

Введение

На сегодняшний день существует множество качественных и количественных подходов к оценке рисков информационной безопасности (ИБ). Их применение позволяет обеспечить требуемый уровень защищенности информационной системы за счет выбора эффективных контрмер.

Международные стандарты, национальные стандарты Российской Федерации (ГОСТ Р ИСО/МЭК 15408, 27001-27005, 13335, 18045, СТО БР ИББС и др.), руководящие документы Федеральной службы по техническому и экспертному контролю (ФСТЭК) России содержат ряд рекомендаций по оценке информационных рисков. Вместе с тем, ввиду высокой неопределённости и сложности процедуры формализации факторов, влияющих на итоговые показатели защищенности системы [1, 2], проблема оценки рисков ИБ остается открытой и требует применения подходов на основе технологий интеллектуального анализа данных и когнитивного моделирования.

В статье рассматриваются следующие подходы к формированию оценки рисков ИБ на основе экспертных оценок и данных проведенного аудита:

1) сети Байеса на основе графа атак [3];
2) нечеткие когнитивные карты [4];
3) нечеткие серые когнитивные карты [5].

Эти подходы объединяет возможность получения интегральной оценки рисков ИБ на основе вероятностного подхода и когнитивного моделирования.

Целью исследования является сравнительный анализ методов когнитивного моделирования при оценке рисков ИБ на основе построения модели атакующих действий злоумышленника с применением технологий интеллектуального анализа. Для достижения поставленной цели необходимо выполнить оценку особенностей применения ме-

* Работа выполнена при финансовой поддержке РФФИ, грант № 17-07-00351.

тодов когнитивного моделирования (сеть Байеса на основе графа атак, нечеткие когнитивные карты и нечеткие серые когнитивные карты) для оценки рисков ИБ компьютерной сети на примере.

1. Анализ возможностей когнитивного моделирования с помощью сети Байеса на основе графа атак для оценки рисков информационной безопасности

Графы атак являются инструментом топологического анализа защищенности информационной системы и позволяют учитывать взаимосвязь и свойства объектов информационной системы на основе результатов сканирования сети, модели нарушителя и данных о конфигурации сети (правила фильтрации межсетевого экрана, маршрутизации, обнаружения атак, достижимости хостов и т.д.). Классификация представления графов атак приведена в таблице 1 [6].

Для формирования рассуждений в условиях неопределенности в соответствии с оценками вероятностей событий и связи между событиями удобным является построение на основе condition-oriented dependency графа сетевой модели в виде сети Байеса [7].

Табл. 1.

Классификация графов атак

Название	Описание
state enumeration graph	вершинам соответствуют тройки (s, d, a), где s – источник атаки, d – цель атаки, a – элементарная атака; дуги обозначают переходы из одного состояния в другое
condition-oriented dependency graph	вершинам соответствуют результаты атак, а дугам – элементарные атаки, приводящие к таким результатам
exploit dependency graph	вершины соответствуют результатам атак или элементарным атакам, дуги отображают зависимости между вершинами – условия, необходимые для выполнения атаки и следствие атаки

Сеть Байеса – модель на основе ориентированного графа, где узлы представляют случайные величины, а направленные ребра – зависимости между ними, образуя направленный граф атак [8].

Совместное распределение вероятностей для текущего узла и родительских узлов можно записать в виде (1):

$$P(X)=\prod_{i=1}^{n} P\left(X_i \middle| parents(X_i)\right), \qquad (1)$$

где $X=\{X_1,...,X_n\}$ множество случайных величин (непрерывных или дискретных) и для каждого узла X_i имеется направленное ребро от каждого узла в паре родительских узлов X_i, указывающее на X_i.

Такая графическая модель может использоваться для оценки рисков ИБ информационной системы с помощью когнитивного моделирования. Каждой вершине графа атак соответствует узел компьютерной сети, которому соответствует значение вероятности достижения этой вершины злоумышленником. Эти оценки выставляются в соответствии с базой системы оценки общей уязвимости CVSS 2.0, в которой численно характеризуется уязвимость по различным параметрам [9-12].

В качестве иллюстрации использования сети Байеса для оценки риска ИБ с применением когнитивного моделирования рассмотрим пример из [3].

Рассмотрим компьютерную сеть (Рисунок 1а), в которой сервер $Host_1$ имеет доступ к передаче и приему файлов по протоколам File Transfer Protocol (FTP), Secure Shell (SSH) и Remote Shell (RSH), а сервер $Host_2$ имеет доступ к передаче и приему данных по протоколам FTP и RSH. Межсетевой экран пропускает трафик по протоколам FTP, SSH и RSH с рабочей станции пользователя $Host_0$ на оба сервера и блокирует весь остальной трафик. Цель злоумышленника – получить права администратора (root) на $Host_2$.

На графе атак (Рисунок 1б) условия *c* представлены в виде эллипсов, в которых в круглых скобках указан задействованный узел сети. Уязвимости *e* отображаются в прямоугольниках, указывая в нижнем индексе на исходный и конечный узел, где первое число отображает источник, второе – назначение.

На рисунке 1б, видно, что для атакующего существует три возможных пути проведения атаки. Один из путей атаки начинается с использования переполнения буфера SSH с $Host_0$ на $Host_1$ ($ssh\_bof_{0,1}$), что дает злоумышленнику возможность выполнять произвольный код на $Host_1$ в роли обычного пользователя. Затем злоумышленник использует уязвимость FTP на $Host_2$ ($ftp\_rhosts_{1,2}$) для анонимной загрузки списка доверенных хостов. Это позволяет злоумышленнику удаленно выполнять команды оболочки на $Host_2$ без предоставления пароля. Использование локального переполнения буфера на $Host_2$ ($local\_bof_{2,2}$) повышает привилегии злоумышленника до уровня администратора на этом сервере.

Вероятности того, что злоумышленник может успешно использовать уязвимости в сети получе-

ны на основе «Base Score» из базы уязвимостей CVSS 2.0, и составляют: $p(ftp\_rhosts) = 0.8$, $p(sshd\_bof) = 0.1$, $p(rsh) = 0.9$ и $p(local\_bof) = 0.1$. Вероятности выполнения условий в этом подходе принимаются равными 1.

Финальная вероятность достижения злоумышленником вершины $P(root_2)$ равна:

$$P(root_2) = P(local\_bof_{2,2}) = 0.087.$$

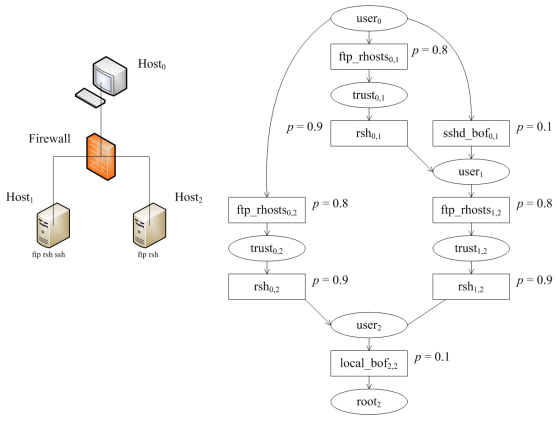

Рис. 1. Конфигурация сети и граф атак

Расчет данным методом позволяет получить вероятностную оценку, непосредственно пригодную определения рисков ИБ для целевого актива. Недостатком такого подхода является сложность масштабирования, так как для больших корпоративных информационных систем необходим переход к приближенным вероятностным выводам.

2. Анализ возможностей когнитивного моделирования оценки рисков ИБ с помощью нечетких когнитивных карт

Нечеткая когнитивная карта, используемая для анализа информационных рисков, представляет собой кортеж множеств (2) [4, 13]:

$$\text{НКК} = \{C, F, W\}, \qquad (2)$$

где C – множество вершин (концептов), F – множество связей между концептами, W – множество весов этих связей.

Для установления силы (веса) связей между концептами используются нечеткие отношения на шкале [0, 1], задаваемые в виде термов лингвистической переменной или с помощью числовых значений на той же шкале [0, 1]. В данной задаче веса w_{ij} соответствуют значениям уязвимостей элементов топологии сети. P_{act} – вероятность активации входного концепта.

Рассмотрим нечеткую когнитивную карту (рисунок 2), построенную на топологии сети, представленной в примере, рассмотренном выше. Здесь внешний пользователь – атакующий, он представлен концептом 1, а целевой узел – концептом 7.

Веса связей между узлами взяты из предыдущего примера, однако в некоторых вариантах расчетов [14, 15] весовые коэффициенты получают с помощью экспертной оценки.

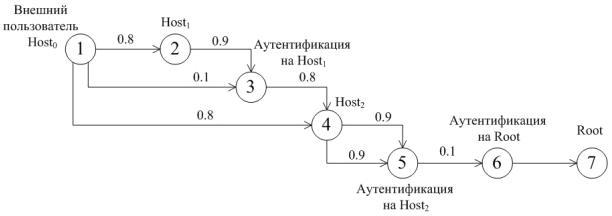

Рис. 2. Нечеткая когнитивная карта

Значение $P_{act} = 0.7$, т.к. действие осуществляется внешним пользователем.

Рассмотрено три сценария действий атакующего (рисунок 3а-в).

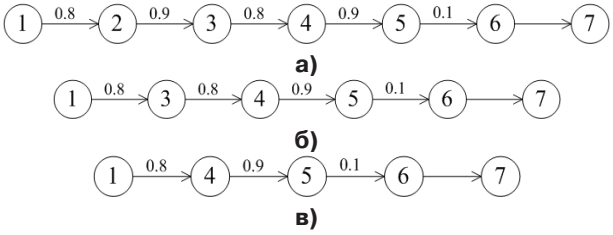

Рис. 3. Сценарии атакующих действий

Вероятности реализации этих сценариев принимает следующие значения: $P_1 = 0.0363$, $P_2 = 0.0403$, $P_3 = 0.0504$.

Вероятность атаки на целевой объект равна:

$$P = \max\{P_j\}.$$

Недостаток НКК – необходимость ввода оценки «Вероятность активации входного концепта». Данная экспертная оценка существенно влияет на финальную оценку рисков ИБ, а также отсутствует в двух других рассматриваемых методиках расчётах рисков ИБ. Вторым недостатком является невозможность комплексно оценить влияние нескольких факторов на один узел. Для такого случая используется операция поиска максимума среди весов влияния, что не всегда отражает вероятность реализации атаки на данный узел.

3. Анализ возможностей когнитивного моделирования оценки рисков ИБ с помощью нечетких серых когнитивных карт

Серая нечеткая когнитивная карта – это модель, состоящая их трех множеств (3) [5, 16]:

$$\text{НСКК} = \{C, F, W\}, \quad (3)$$

где $C = \{C_i\}$ – множество концептов (вершин графа) ($i \in [1, n]$); $F = \{F_{ij}\}$ – множество отношений связей между концептами (дуги графа); $W = \{W_{ij}\}$ – множество отношений межу концептами, определяющих веса связей $(i, j) \in \Omega$ где Ω – множество пар смежных концептов.

Отличием НСКК от обычных НКК является способ задания оценки весов связи с помощью «серых» интервальных чисел $\otimes W_{ij}$. Эти числа определяются следующим образом (4):

$$\otimes W_{ij} \in [\underline{W_{ij}}, \overline{W_{ij}}],\ \{\underline{W_{ij}}, \overline{W_{ij}}\} \in [-1, 1], \quad (4)$$

где $\underline{W_{ij}}$ – нижняя граница серого числа, а $\overline{W_{ij}}$ – верхняя граница серого числа.

Нечеткая серая когнитивная карта для рассматриваемой топологии сети представлена на рисунке 4:

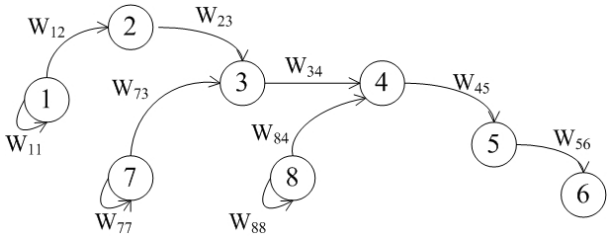

Рис. 4. Нечеткая серая когнитивная карта

Концепт C_1 – угроза доступа внешнего пользователя к $Host_1$, C_2 – $Host_1$, концепт C_3 представляет собой процедуру аутентификации на $Host_1$, концепт C_4 – $Host_2$, C_5 – аутентификация на $Host_2$, C_6 – получение прав администратора на $Host_2$. C_7 – угроза аутентификации на $Host_1$, концепт C_8 – угроза доступа к $Host_2$. Концепты C_1, C_7 и C_8 в [17] называются драйверами.

Веса связей взяты из примера, но представлены в таблице 2 в виде «серых» чисел.

Табл. 2.

Значения весов

Вес	Значение веса связи	«Серость»
W_{12}	[0.7; 0.9]	0.1
W_{23}	[0.85;0.95]	0.05
W_{73}	[0.05;0.2]	0.075
W_{84}	[0.7;0.9]	0.1
W_{34}	[0.7; 0.9]	0.1
W_{45}	[0.85;0.95]	0.05
W_{56}	[0.05;0.2]	0.075

Значения «серости» оценки вычисляются по формуле (5):

$$\Phi(\otimes W_{ij}) = \frac{\left|\overline{W_{ij}} - \underline{W_{ij}}\right|}{2} \quad (5)$$

Рассмотрим три сценария атаки.

Первый сценарий представлен на рисунке 5.

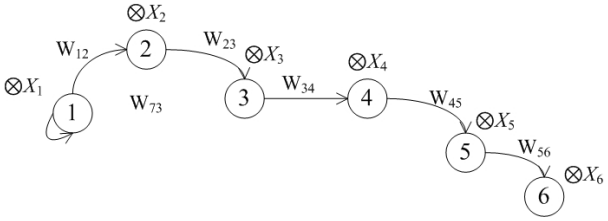

Рис. 5. Первый сценарий атаки

Произведем оценку верхней и нижней границы X_6. Начальные условия для $X_2 - X_6 = \{0,0\}$, а X_1 как оценка генератора, имеет оценку $\{0.8, 1\}$. Тогда рассчитаем значения оценок состояния. Расчётные установившиеся значения для верхних и нижних границ достигаются за 10 тактов.

Серый вектор для сценария 1 получился следующим:

$$\otimes X_A =$$

$$= \{[0.8; 1], [0.37; 0.51], [0.24; 0.41], [0.2; 0.33], [0.073; 0.062]\}$$

Искомые значения для концепта C_6 будут определяться серым числом $\otimes X_6 \in [0.0073; 0.062]$.

Сценарии 2 и 3 изображены на рисунке 6.

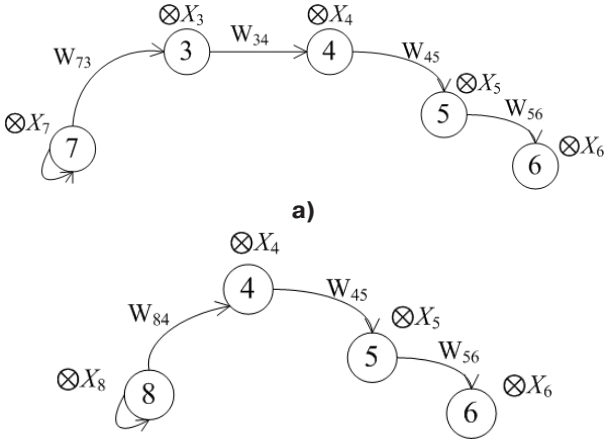

Рис. 6. Второй (а) и третий (б) сценарии атаки

После выполнения аналогичных расчетов для сценариев 2 и 3 получаем:

Сценарий 2: $\otimes X_6 \in [0.015; 0.083]$.

Сценарий 3: $\otimes X_6 \in [0.017; 0.086]$.

Интегральное значение оценки рисков ИБ вследствие получения прав администратора на $Host_2$ примем как среднее арифметическое сценариев 1-3:

$$\otimes X_6 \in [0.011; 0.077]$$

Данный метод позволяет учесть фактор неопределенности, возникающий в процессе оценки

вероятности уязвимости каждого из узлов ИБ и, в отличии от НКК, позволяет оценивать комплексное влияние нескольких факторов на один узел информационной сети в каждом из сценариев атак.

3. Сравнительная характеристика возможностей когнитивного моделирования при оценке рисков ИБ

Преимущества байесовского подхода для оценки рисков ИБ в использовании априорных вероятностей, которые затем уточняются с помощью выборочных данных. Можно выделить следующие недостатки: предполагается известность априорного распределения вероятностей известно до начала наблюдений и не предлагается способов его выбора. Принятие решения в больших моделях требует больших вычислительных затрат, связанных с численным интегрированием в многомерных пространствах, и требует перехода к приближенным вероятностным выводам [18-20].

НКК и НСКК обладает наглядностью, интерпретируемостью и способностью к обучению на реальных данных. Применение НСКК позволяет перейти от «точечных» оценок мнений экспертов к интервальным оценкам и к получению интервальных оценок конечных результатов, что является более достоверным. Интервальные оценки весов НСКК могут отражать разброс мнений группы экспертов, что позволяет более полно учесть имеющиеся для анализа риска данные. Когнитивное моделирование оценки рисков ИБ с помощью НКК и НСКК позволяет учесть фактор неопределенности, возникающий в процессе оценки вероятности уязвимости каждого из узлов ИБ. Недостатком НКК является необходимость ввода экспертной оценки «Вероятность активации входного концепта», которая существенно влияет на финальную оценку риска информационной безопасности.

Сравнительный анализ когнитивного моделирования оценки рисков ИБ с использованием Байесовской сети, НКК и НСКК приведены в таблице 5.

Основной проблемой при использовании рассмотренных методов когнитивного моделирования является недостаточный объем статистической информации об угрозах и уязвимостях и/или его противоречивость и неполнота, что затрудняет формирование достоверных оценок рисков ИБ и приводит к существенному влиянию качества экспертных оценок, полученных в процессе аудита ИБ, на итоговые результаты.

Табл. 5.
Сравнительная характеристика методов оценки рисков ИБ

Критерий	Байесовская сеть	НКК	НСКК
Простота использования	Низкая	Средняя	Средняя
Интерпретируемость результатов	Выше средней	Средняя	Средняя
Сложность вычислительной реализации	Высокая	Средняя	Выше средней
Согласованность оценок с другими подходами	Выше средней	Высокая	Высокая
Применимость к организации (объекту защиты) разного размера и области деятельности	Средняя	Выше средней	Выше средней
Удобство применения методики и наличие ПО	Выше средней	Средняя	Средняя
Удобство восприятия результатов оценки	Среднее	Выше средней	Выше средней

Литература

1. *Teixeira A., van Gelder P.* Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications // 11th International Conference on Critical Information Infrastructures Security, CRITIS 2016, Paris, France, October 10–12, 2016, Revised Selected Papers. Springer, 2017. – Т. 10242. – 50 p.
2. *Kriaa S. et al.* A survey of approaches combining safety and security for industrial control systems // Reliability engineering & system safety. – 2015. – Т. 139. – С. 156-178.
3. *Munoz-González L. et al.* Exact inference techniques for the analysis of Bayesian attack graphs // IEEE Transactions on Dependable and Secure Computing. – 2017. – Т. 16. – №. 2. – С. 231-244.

4. *Васильев В.И., Вульфин А.М., Кудрявцева Р.Т.* Анализ и управление рисками информационной безопасности с использованием технологии когнитивного моделирования // Доклады ТУСУРа. – 2017. – Т. 20. – №. 4. – С. 61-66.
5. *Васильев В.И., Вульфин А.М., Гузаиров М.Б., Кириллова А.Д.* Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт // Информационные технологии. – 2018. – 10(24). – С. 657-664.
6. *Алексеев Д.М., Иваненко К.Н., Убирайло В.Н.* Построение графа атак для анализа защищенности компьютерных сетей // Символ наук. – 2016. – 7-2.– С. 31-34.
7. *Mell P., Harang R.* Minimizing Attack Graph Data Structures // Tenth International Conference on Software Engi-neering Advances, (Barcelona, Spain). 2015. – С. 376-385.
8. *Friedman N., Geiger D., Goldszmidt M.* Bayesian network classifiers // Machine learning. – 1997. – Т. 29. – № 2-3. – С. 131-163.
9. *Scarfone K., Mell P.* An analysis of CVSS version 2 vulnerability scoring // Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement. IEEE Computer Society, 2009. – С. 516-525.
10. *Котенко И.В.* Методика выбора контрмер в системах управления информацией и событиями безопасности. Информационно-управляющие системы. СПб.: Политехника. – 2015. – Т. 3. – С. 60-69.
11. *Котенко И.В.* Система оценки уязвимостей CVSS и ее использование для анализа защищенности компьютерных систем. Защита информации. Инсайд. – 2011. – Т. 5. – С. 54-60.
12. *Дойникова Е.В., Котенко И.В.* Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер. Информационная безопасность. – 2018. – 2(57). – С. 211-240.
13. *Siraj A., Bridges S.M., Vaughn R.B.* Fuzzy cognitive maps for decision support in an intelligent intrusion detection system // Joint 9th IFSA World Congress and 20th NAFIPS International Conference: Proceedings: July 25-28, 2001, Vancouver, British Columbia, Canada. – Т. 4. – С. 2165-2170.
14. *Гузаиров М.Б., Машкина И.В., Степанова Е.С.* Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности // Безопасность информационных технологий. – 2011. – 2(18). – С. 37-49.
15. *Mashkina, I.V. et al.* Issues of information security control in virtualization segment of company information system // Proceedings of the XIX International Conference on Soft Computing and Measurements SCM'2016. St. Petersburg: IEEE, 2016. – С. 161-163.
16. *Salmeron, J.L.* Modelling grey uncertainty with fuzzy grey cognitive maps // Expert Systems with Applications. – 2010. – 12(37). – С. 7581-7588.
17. *Knight Ch.J.K., Lloyd D.J.B., Penn A.S.* Linear and Sigmoidal Fuzzy Cognitive Maps: An Analysis of Fixed Points. Available at: www.inescid.pt/indicators/Ficherous/175.pdf (accessed March 26, 2019).
18. *Boutalis Y., Kottas T., Christodoulou M.* On the existence and uniqueness of solutions for the concept values in fuzzy cognitive maps // 47th IEEE Conference on Decision and Control, Cancun: IEEE, 2008. – С. 98-104.
19. *Звягин Л.С.* Применение байесовского подхода в измерениях аналитических данных как фактор формирования процессов системного экономического развития // Молодой ученый. – 2017. – Т. 22. – С. 256-261.
20. *Shin, J. et al.* Development of a cyber security risk model using Bayesian networks // Reliability Engineering & System Safety. – 2015. – Т. 134. – С. 208-217.

Гузаиров Мурат Бакеевич. Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет» (ФГБОУ ВО «УГАТУ»), г. Уфа, Россия. Профессор кафедры вычислительной техники и защиты информации, доктор технических наук, профессор. Количество печатных работ: более 100. Область научных интересов: системный анализ, управление в социальных и экономических системах. E-mail: guzairov@ugatu.su

Вульфин Алексей Михайлович. Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет» (ФГБОУ ВО «УГАТУ»), г. Уфа, Россия. Доцент кафедры вычислительной техники и защиты информации, кандидат технических наук. Количество печатных работ: более 50. Область научных интересов: интеллектуальный анализ данных и моделирование сложных технических систем. E-mail: vulfin.alexey@gmail.com

Картак Вадим Михайлович. Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет» (ФГБОУ ВО «УГАТУ»), г. Уфа, Россия. Заведующий кафедрой вычислительной техники и защиты информации, доктор физико-математических наук, доцент. Количество печатных работ: более 50. Область научных интересов: информационная безопасность, методы оптимизации. E-mail: kvmail@mail.ru

Кириллова Анастасия Дмитриевна. Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет» (ФГБОУ ВО «УГАТУ»), г. Уфа, Россия. Аспирант кафедры вычислительной техники и защиты информации. Количество печатных работ: 17. Область научных интересов: комплексный анализ и управление рисками кибербезопасности АСУ ТП промышленных объектов с использованием технологии когнитивного моделирования. E-mail: kirillova.andm@gmail.com

Миронов Константин Валерьевич. Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет» (ФГБОУ ВО «УГАТУ»), г. Уфа, Россия. Старший преподаватель кафедры вычислительной техники и защиты информации, PhD. Количество печатных работ: 20. Область научных интересов: применение распределенного реестра в системах промышленного интернета вещей с ограниченными вычислительными ресурсами. E-mail: mironovconst@gmail.com

Comparative analysis of algorithms for cognitive modeling in assessing information security risks

M.B. Guzairov[1], A.M. Vulfin[1], V.M. Kartak[1], A.D. Kirillova[1], K.V. Mironov[1]

[1] Ufa State Aviation Technical University, Ufa, Russia

Abstract. The article discusses the use of approaches to the assessment of information risks of a computer network based on data mining and cognitive modeling. Analyzed the main stages of the implementation of information security risk assessment using the Bayesian network based on the graph of attacks, fuzzy cognitive maps and fuzzy gray cognitive maps, formulated recommendations for their use.

Keywords*: information security, risk assessment, Bayesian network, fuzzy cognitive maps, fuzzy gray cognitive maps*

DOI: 10.14357/20790279190408

References

1. *Teixeira, A., van Gelder P.* 2017. Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications. 11th International Conference on Critical Information Infrastructures Security, CRITIS 2016, Paris, France, October 10–12, 2016, Revised Selected Papers. Springer, 2017. Vol. 10242. 50 p.
2. *Kriaa, S. et al.* 2015. A survey of approaches combining safety and security for industrial control systems. Reliability engineering & system safety. 139: 156–178.
3. *Munoz-González, L. et al.* 2017. Exact inference techniques for the analysis of Bayesian attack graphs. IEEE Transactions on Dependable and Secure Computing. 16.2 (2017): 231–244.
4. *Vasilyev, V.I., A.M. Vulfin, R.T. Kudrjavceva.* 2017. Analiz i upravlenie riskami informacionnoj bezopasnosti s ispol'zovaniem tehnologii kognitivnogo modelirovanija [Analysis and management of information security risks using cognitive modeling technology]. Doklady TUSURa, 4(20): 61–66.
5. *Vasilyev, V.I., A.M. Vulfin, M.B. Guzairov, A.D. Kirillova.* 2018. Interval'noe ocenivanie informacionnyh riskov s pomoshh'ju nechetkih seryh kognitivnyh kart [Interval estimation of information risks with use of Fuzzy Grey Cognitive Maps]. Informacionnye tehnologii, 10(24): 657–664.
6. *Alekseev, D.M., K.N. Ivanenko, V.N.* Ubirajlo. 2016. Postroenie grafa atak dlja analiza zashhishhennosti komp'juternyh setej [Build a graph of attacks to analyze the security of computer networks]. Simvol nauki, 7-2: 31–34.
7. *Mell, P., R. Harang.* 2015. Minimizing Attack Graph Data Structures. In the Tenth International Conference on Software Engineering Advances, Barcelona, Spain, 2015: 376–385.
8. *Friedman, N., D. Geiger and M. Goldszmidt.* 1997. Bayesian network classifiers. Machine learning. 2-3(29): 131–163.
9. *Scarfone, K., P. Mell.* 2009. An analysis of CVSS version 2 vulnerability scoring. Proceedings of the 2009 3rd International Symposium on Empirical

Software Engineering and Measurement. IEEE Computer Society, 2009: 516–525.
10. *Kotenko, I.V.* 2015. Metodika vybora kontrmer v sistemah upravlenija informaciej i sobytijami bezopasnosti [Method of choosing countermeasures in information security and event management systems]. Informacionno-upravljajushhie sistemy. SPb.: Politehnika. 3: 60–69.
11. *Kotenko, I.V.* 2011. Sistema ocenki ujazvimostej CVSS i ee ispol'zovanie dlja analiza zashhishhennosti komp'juternyh sistem [CVSS vulnerability assessment system and its use for computer systems security analysis]. Zashhita informacii. Insajd. 5: 54–60.
12. *Dojnikova, E.V., I.V. Kotenko.* 2018. Sovershenstvovanie grafov atak dlja monitoringa kiberbezopasnosti: operirovanie netochnostjami, obrabotka ciklov, otobrazhenie incidentov i avtomaticheskij vybor zashhitnyh mer [Improving attack graphs to monitor cybersecurity: handling inaccuracies, processing loops, displaying incidents, and automatic selection of protective measures]. Informacionnaja bezopasnost', 2(57): 211–240.
13. *Siraj, A., S.M. Bridges and R.B. Vaughn.* 2001. Fuzzy cognitive maps for decision support in an intelligent intrusion detection system. In Joint 9th IFSA World Congress and 20th NAFIPS International Conference: Proceedings: July 25-28, 2001, Vancouver, British Columbia, Canada. 4: 2165–2170.
14. *Guzairov, M.B., I.V. Mashkina, E.S. Stepanova.* 2011. Postroenie modeli ugroz s pomoshh'ju nechetkih kognitivnyh kart na osnove setevoj politiki bezopasnosti [Building a threat model using fuzzy cognitive maps based on network security policy]. Bezopasnost' informacionnyh tehnologij. 2(18): 37–49.
15. *Mashkina, I.V. et al.* 2016. Issues of information security control in virtualization segment of company information system. In Proceedings of the XIX International Conference on Soft Computing and Measurements SCM'2016. St. Petersburg: IEEE, 2016:161–163.
16. *Salmeron, J.L.* 2010. Modelling grey uncertainty with fuzzy grey cognitive maps. Expert Systems with Applications, 12(37): 7581–7588.
17. *Knight, Ch.J.K., D.J.B. Lloyd and A.S.* Penn Linear and Sigmoidal Fuzzy Cognitive Maps: An Analysis of Fixed Points. Available at: www.inescid.pt/indicators/Ficherous/175.pdf (accessed March 26, 2019).
18. *Boutalis, Y., T. Kottas, M. Christodoulou.* 2008. On the existence and uniqueness of solutions for the concept values in fuzzy cognitive maps. 47th IEEE Conference on Decision and Control, Cancun: IEEE, 2008: 98–104.
19. *Zvjagin, L.S.* 2017. Primenenie bajesovskogo podhoda v izmerenijah analiticheskih dannyh kak faktor formirovanija processov sistemnogo jekonomicheskogo razvitija [The use of the Bayesian approach in the measurement of analytical data as a factor in the formation of processes of systemic economic development]. Molodoj uchenyj, 22: 256–261.
20. *Shin, J. et al.* 2015. Development of a cyber security risk model using Bayesian networks. Reliability Engineering & System Safety. 134: 208–217.

M.B Guzairov. Doctor of Technical Science, Professor of the Department of Computer science and information security, Ufa State Aviation Technical University, K.Marks St. 12, Ufa, 450008, Russian Federation;
E-mail: guzairov@ugatu.su.

A.M. Vulfin. PhD (Cand. of Sc.) Ass. Professor of the Department of Computer science and information security, Ufa State Aviation Technical University, K.Marks St. 12, Ufa, 450008, Russian Federation;
e-mail: vulfin.alexey@gmail.com

V.M. Kartak. Doctor of Technical Science, Professor of the Department of Computer science and information security, Ufa State Aviation Technical University, K.Marks St. 12, Ufa, 450008, Russian Federation;
E-mail: kvmail@mail.ru

A.D. Kirillova. Postgrad. Student of the Department of Computer science and information security, Ufa State Aviation Technical University, K.Marks St. 12, Ufa, 450008, Russian Federation;
E-mail: kirillova.andm@gmail.com

K.V. Mironov. PhD, Senior lecturer of the Department of Computer science and information security, Ufa State Aviation Technical University, K.Marks St. 12, Ufa, 450008, Russian Federation; E-mail: mironovconst@gmail.com