ISSN 1992-6502 (Print) Вестник УГАТУ ISSN 2225-2789 (Online)
2019. Т. 23, № 4 (86). С. 122–131 http://journal.ugatu.ac.ru

УДК 004.056

АНАЛИЗ РИСКОВ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ТЕЛЕМЕТРИЧЕСКОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ КОГНИТИВНОГО МОДЕЛИРОВАНИЯ

В. И. Васильев[1], А. М. Вульфин[2], В. В. Берхольц[3], А. Д. Кириллова[4], С. М. Бельский[5]

[1] vasilyev@ugatu.ac.ru, [2] vulfin.alexey@gmail.com, [3] torina4@yandex.ru, [4] kirillova.andm@gmail.com, [5]1902199615@mail.ru

ФГБОУ ВО «Уфимский государственный авиационный технический университет» (УГАТУ)

Поступила в редакцию 07.05.2019

Аннотация. Рассмотрены вопросы анализа рисков обеспечения целостности телеметрической информации о состоянии бортовых подсистем летательного аппарата. Предложена методика оценки защищенности системы сбора, хранения и обработки телеметрической информации на основе технологии когнитивного моделирования с использованием нечетких серых когнитивных карт. Разработано программное средство «Cognitive Map Constructor» для автоматизации процесса анализа и управления рисками.

Ключевые слова: информационная безопасность; оценка рисков; целостность информации; нечеткая серая когнитивная карта.

ВВЕДЕНИЕ

Как свидетельствует статистика последних лет [1, 2], промышленные предприятия сегодня все чаще становятся объектом целенаправленных кибератак со стороны хакеров, скоординированных бот-сетей, нечестных конкурентов, субъектов промышленного шпионажа и т.д. Характерной особенностью современных промышленных систем автоматизации и контроля технологических процессов (АСУ ТП) является не только резкое усложнение их информационной инфраструктуры (оборудование, ПО, сети), но и неизбежность контакта с внешним миром (подрядчики, разработчики, системные интеграторы, поставщики облачных решений и т.д.). Все это делает ключевой элемент предприятия – АСУ ТП чрезвычайно уязвимым по отношению к потенциальным внешним и внутренним злоумышленным действиям и поэтому заслуживает пристального и безотлагательного внимания со стороны специалистов. Наиболее существенные шаги в решении проблемы обеспечения информационной безопасности АСУ ТП (а в последнее время все чаще говорят об обеспечении кибербезопасности АСУ ТП) предпринимаются по пути разработки серии соответствующих международных и национальных стандартов, регулирующих терминологию, базовые подходы и рекомендации по обеспечению определенных требований к обеспечению кибербезопасности промышленных автоматизированных систем (NIST SP 800-82, NERC CIP, ISA/IEC 62443, ГОСТ Р МЭК 62443) [3–5].

Говоря о вопросах обеспечения информационной безопасности и кибербезопасности АСУ ТП, следует иметь в виду одно важное различие между этими ключевыми понятиями [3]. Если в задачах информаци-

Работа поддержана грантом РФФИ № 17-07-00351А и № 18-00-00238КОМФИ

онной безопасности в качестве объекта защиты выступает корпоративная информационная система (КИС), а защищаемым ресурсом является информация, подлежащая обработке, хранению и передаче в системе, и основная цель – обеспечить ее конфиденциальность, то с точки зрения кибербезопасности главным защищаемым ресурсом является уже сам технологический процесс, а основная цель – обеспечить его непрерывность (т.е. доступность всех узлов) и целостность (в том числе передаваемой между узлами информации).

В основе указанных выше стандартов (и прежде всего стандартов ISA/IEC 62443 и ГОСТ Р МЭК 62443) используется риск-ориентированный подход, позволяющий сформировать необходимый комплекс требований к обеспечению безопасности АСУ ТП конкретного предприятия на основе детального изучения задействованных в этой системе информационных активов и последующего анализа цепочки «угрозы – уязвимости – ущерб (риски)», с выработкой рекомендаций по обеспечению допустимого уровня риска. Особо отмечается необходимость разработки и использования на данном этапе математических моделей и методов качественной и количественной оценки рисков обеспечения кибербезопасности АСУ ТП, применение которых позволит повысить оперативность и достоверность принимаемых управленческих решений.

На сегодняшний день известно большое количество методик оценки информационных рисков, таких как OCTAVE, CRAMM, RiskWatch, COBRA, MIST, «АванГард», ГРИФ и др. [6, 7]. Вместе с тем ввиду высокой степени неопределенности и сложности процедуры формализации факторов, влияющих на итоговые показатели защищенности системы (особенно для таких сложных объектов, как АСУ ТП), проблема оценки рисков остается открытой и требует разработки и применения новых подходов, из которых в последние годы хорошо зарекомендовали себя методы и технологии интеллектуального анализа данных и когнитивного моделирования [8–11]. В качестве базового инструмента исследования при этом обычно используются различные разновидности нечетких когнитивных карт (НКК) – классические НКК Б. Коско, НКК Силова, реляционные НКК, продукционные НКК и др. Ниже для решения поставленной задачи оценки информационных рисков АСУ ТП мы воспользуемся аппаратом нечетких серых когнитивных карт (НСКК), впервые предложенным в 2010 г. Хосе Салмероном [12]. Первая попытка применения данного подхода для решения задачи интервального оценивания информационных рисков делалась авторами в [13], где было показано, что использование НСКК позволяет более полно учесть фактор неопределенности, возникающий в процессе оценки вероятности использования уязвимости каждой из компонент информационной системы.

Нечеткая серая когнитивная карта – это модель в форме ориентированного графа, состоящая из трех множеств:

$$\text{НСКК} = \{C, F, W\}, \qquad (1)$$

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

Отличием НСКК от обычных нечетких когнитивных карт (НКК) является задание оценок весов связей с помощью «серых» (интервальных) чисел $\otimes W_{ij}$. Эти числа определяются следующим образом:

$$\otimes W_{ij} \in [\underline{W}_{ij}, \overline{W}_{ij}], \{\underline{W}_{ij}, \overline{W}_{ij}\} \in [-1,1], \qquad (2)$$

где $\underline{W}_{ij}$ – нижняя граница серого числа; $\overline{W}_{ij}$ – верхняя граница серого числа. Применение НСКК позволяет перейти от «точечных» оценок мнений экспертов к интервальным (размытым) оценкам и, как следствие, к получению интервальных оценок конечных результатов, что представляется более логичным и достоверным. Интервальные оценки весов НСКК могут отображать разброс мнений группы экспертов, привлекаемых к процедуре анализа рисков.

Целью настоящего исследования является разработка методики количественной оценки рисков на примере задачи обеспече-

ния целостности телеметрической информации (ТМИ) на предприятии-изготовителе изделий авиационной техники с использованием технологии многослойных (вложенных) НСКК. В качестве исследуемого объекта защиты рассматривается автоматизированная информационная система (АИС), предназначенная для сбора, хранения и обработки информации о параметрах состояния авиационных бортовых систем, получаемой от наземных служб технического обслуживания в течение всего периода их эксплуатации.

СТРУКТУРНАЯ СХЕМА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ СБОРА, ХРАНЕНИЯ И ОБРАБОТКИ ТМИ

Обобщенная структура защищенной территориально распределенной модульной системы сбора, хранения и обработки ТМИ, предложенная в [14, 15], представлена на рис. 1.

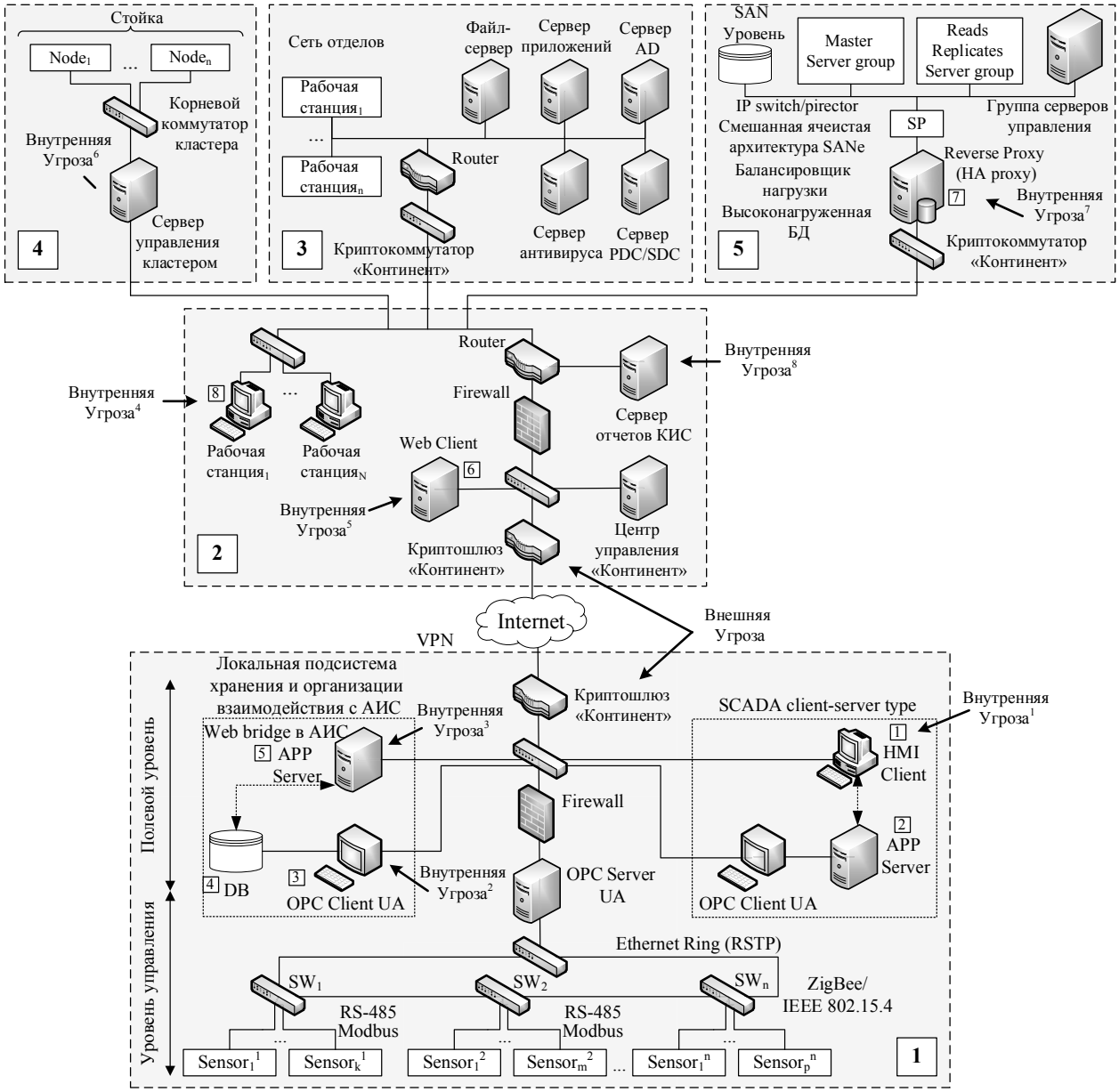

Рис. 1. Обобщенная структурная схема защищенной системы сбора, хранения и обработки ТМИ

В составе АИС можно выделить следующие подсистемы (зоны), объединяемые по принципу единства выполняемых функций и требований к безопасности их реализации:

 Подсистема сбора и хранения данных на станциях обслуживания (Зона 1), включающая в себя:

Элемент 1 – клиентская часть Web-base SCADA системы;

Элемент 2 – серверная часть Web-base SCADA системы;

Элемент 3 – OPC UA клиент;

Элемент 4 – временное хранилище для размещения оперативных данных телеметрии, накапливаемых на объекте;

Элемент 5 – серверная часть системы передачи накопленных данных в хранилище ПИ;

 Подсистема хранения ТМИ с функциями отказоустойчивости (Зона 2), где:

Элемент 7 – узел доступа к хранилищу данных ТМИ на ПИ;

 Подсистема обработки данных ТМИ с помощью иерархии математических моделей СТИ (зоны 3, 4);

 Подсистема поддержки и реализации бизнес-процессов ПИ (Зона 5);

 Ядро корпоративной информационной сети (КИС) предприятия-изготовителя (Зона 0), где:

Элемент 6 – клиентская часть для организации доступа к серверу станции обслуживания с целью передачи накопленных оперативных данных ТМИ в хранилище ПИ;

Элемент 8 – АРМ администратора и обслуживающего персонала ядра КИС ПИ;

Рассмотрим задачу анализа рисков, связанных с обеспечением целостности ТМИ вследствие возможных угроз на представленную АИС.

НЕЧЕТКАЯ СЕРАЯ КОГНИТИВНАЯ КАРТА ДЛЯ ОЦЕНКИ РИСКОВ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ТМИ В АИС

Укрупненная исходная НСКК для рассматриваемой АИС сбора, хранения и обработки ТМИ с учетом выделенных зон представлена на рис. 2.

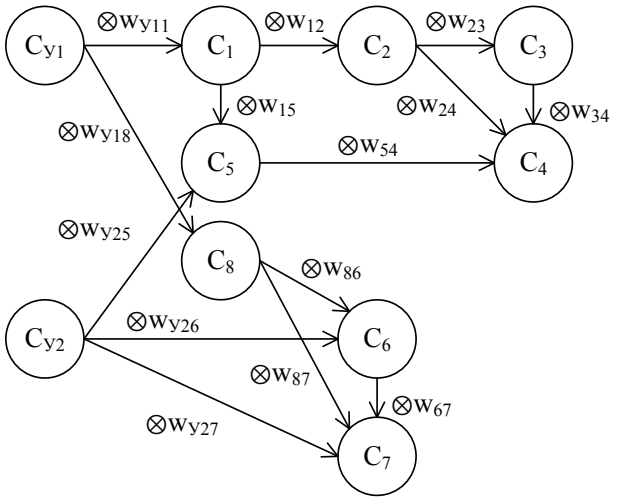

Рис. 2. Укрупненная НСКК для оценки рисков АИС

Здесь: концепт C_{y_1} – внутренняя угроза целостности ТМИ (например, вследствие сбоев или ошибочных действий персонала); C_{y_2} – внешняя угроза целостности ТМИ (например, вследствие попытки несанкционированного доступа извне к информации); C_1 – доступ к HMI Client (возможность запуска в браузере клиентской части SCADA системы на основе Web-приложения); C_2 – доступ к оперативным данным ТМИ, которые могут быть модифицированы до внесения в БД на узлах SCADA client-server type; C_3 – доступ к клиенту для взаимодействия с сервером OPC на основе спецификации Unified Architecture; C_4 – доступ к БД хранения оперативных данных ТМИ, которые могут быть несанкционированно модифицированы; C_5 – запуск модуля доступа к БД оперативного хранения ТМИ на станциях обслуживания ЛА; C_6 – доступ к ТМИ из оперативного хранилища станций обслуживания ЛА; C_7 – получение несанкционированного доступа к ТМИ в долгосрочном хранилище; C_8 – несанкционированный доступ к рабочей станции ядра КИС ПИ.

На основании проведенного анализа угроз и уязвимостей АИС сбора, хранения и обработки ТМИ, а также сценариев реализации угроз в системе [15] с использованием графов атак, можно построить комплекс вложенных НСКК для отдельных подсистем АИС, содержащих целевые объекты атаки на ТМИ (рис. 3–6).

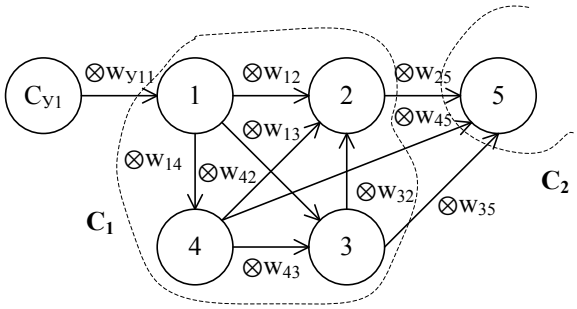

Рис. 3. Декомпозиция концепта C_1 исходной НСКК моделирования запуска в браузере клиентской части SCADA системы на основе Web-приложения

На рис. 3 представлены следующие концепты:

1 – эксплуатация уязвимости системы авторизации ОС;

2 – эксплуатация уязвимости Web-клиента SCADA;

3 – эксплуатация уязвимости браузера ОС для запуска клиентской части SCADA;

4 – эксплуатация уязвимости доступа к памяти ОС;

5 – эксплуатация уязвимости системы авторизации OPC UA клиента.

Состояния концептов C_i характеризуются переменными X_i, принимающими значения в интервале $[0, 1]$:

$$\otimes X_i(k+1) = \\ = f_i(\otimes X_i(k) + \sum_{\substack{j=1 \\ (j\neq i)}}^{n} \otimes w_{ji} \otimes X_j(k)).$$

Функции активации концептов $f_i(\cdot)$ – однополярные сигмоиды (логистические функции): $f_i(X) = 1/(1 + e^{-X})$.

В табл. 1 приведены значения весов связей НСКК, реализующей декомпозицию концепта C_1 исходной НСКК (рис. 3), заданные экспертами.

Таблица 1

Значения весов связей НСКК

Вес связи	*Значение веса связи*	*Серость (разброс оценки)*
w_{y_11}	[0,6; 0,75]	0,075
w_{12}	[0,5; 0,7]	0,1
w_{13}	[0,5; 0,7]	0,1
w_{14}	[0,15; 0,3]	0,075
w_{25}	[0,55; 0,65]	0,05
w_{32}	[0,35; 0,55]	0,1
w_{35}	[0,55; 0,65]	0,05
w_{42}	[0,3; 0,5]	0,1
w_{43}	[0,15; 0,3]	0,075
w_{45}	[0,2; 0,45]	0,125

Проведем расчеты с помощью данной НСКК для сценария реализации угрозы запуска в браузере клиентской части SCADA системы на основе Web-приложения. Для этого выполним оценку изменения верхней и нижней границы переменной состояния X_5 во времени $k = 1, 2, 3, ...$ (табл. 2, 3). Начальные условия для состояния X_{y_1} имеют значение $[0{,}8;1]$, а для $X_1 \div X_5$ – $[0,0]$.

Таблица 2

Верхние границы оценок состояния концептов

k / $\overline{X_i}$	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
$\overline{X_1}$	0,36	0,5	0,55	0,57	0,58	0,58	0,58	0,58
$\overline{X_2}$	0	0,125	0,28	0,4	0,48	0,52	0,54	0,55
$\overline{X_3}$	0	0,125	0,24	0,32	0,36	0,38	0,39	0,4
$\overline{X_4}$	0	0,054	0,1	0,13	0,15	0,16	0,16	0,16
$\overline{X_5}$	0	0	0,093	0,23	0,36	0,45	0,5	0,53

Таблица 3

Нижние границы оценок состояния концептов

k / $\underline{X_i}$	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
$\underline{X_1}$	0,24	0,34	0,39	0,41	0,43	0,43	0,43	0,43
$\underline{X_2}$	0	0,059	0,13	0,18	0,22	0,25	0,27	0,28
$\underline{X_3}$	0	0,059	0,115	0,16	0,18	0,19	0,2	0,2
$\underline{X_4}$	0	0,018	0,034	0,046	0,052	0,058	0,06	0,06
$\underline{X_5}$	0	0	0,034	0,087	0,14	0,18	0,21	0,24

Серый вектор состояния $\otimes X$ для сценария реализации угрозы запуска злоумышленником в браузере клиентской части SCADA системы на основе Web-приложения в результате расчетов получился следующим:

$$\otimes X = \{[0{,}8;\ 1],\ [0{,}43;\ 0{,}58],\ [0{,}28;\ 0{,}55],\\ [0{,}2;\ 0{,}4],\ [0{,}06;\ 0{,}16],\ [0{,}24;\ 0{,}53]\}.$$

Искомые значения для состояния целевого концепта 5 будут определяться серым числом $\otimes X_5 \in [0{,}24;\ 0{,}53]$.

Учитывая, что концепты НСКК подсистем соответствуют узлам графов атак из работы [15], получаем для концепта C_2 (рис. 4, *а*).

10 – целевой концепт доступа к оперативным данным ТМИ, которые могут быть модифицированы до внесения в БД на узлах SCADA client-server type.

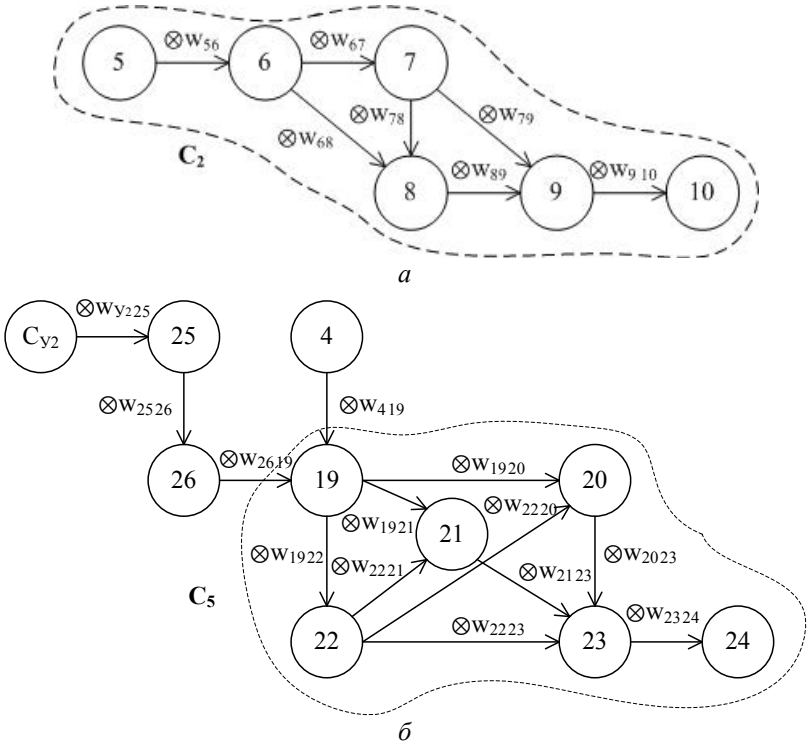

Рис. 4. Декомпозиция концепта: *а* – C_2; *б* – C_5 укрупненной НСКК для оценки рисков АИС

Аналогично для концепта C_5 (рис. 4, *б*) имеем:

24 – целевой концепт несанкционированного запуск модуля доступа к БД оперативного хранения ТМИ на станциях обслуживания ЛА.

Для концептов C_6 и C_7 (рис. 5):

36 – целевой концепт нарушения целостности ТМИ в оперативном хранилище станций ТО ЛА;

40 – целевой концепт нарушения целостности ТМИ в долгосрочном хранилище.

Ввиду значительного объема вычислений при работе с НСКК, содержащими большое количество концептов, необходима разработка программного инструментария для автоматизации когнитивного моделирования с использованием НСКК.

АВТОМАТИЗАЦИЯ АНАЛИЗА И УПРАВЛЕНИЯ РИСКАМИ НА ОСНОВЕ ТЕХНОЛОГИИ КОГНИТИВНОГО МОДЕЛИРОВАНИЯ

С целью решения задачи автоматизации анализа и управления рисками с использованием НСКК было разработано программное средство «Cognitive Map Constructor» [16]. Данное программное средство позволяет строить и редактировать НСКК, проводить с их помощью анализ рисков ИБ и обосновывать выбор состава необходимых контрмер из заданного пользователем набора. В результате строится диаграмма оценки информационных рисков при различных сценариях внедрения контрмер и реализации атак.

Помимо поддержки НСКК с установкой весов связей в виде верхних и нижних границ, программа допускает использование лингвистических термов нечеткой логики, а также задание весов в виде только «белых» четких чисел. Программа имеет интерфейс, реализованный на языке гипертекстовой разметки HTML с применением CSS, позволяющий отображать НСКК и необходимую сопроводительную информацию по концептам и связям, и способна работать на любой графической операционной системе, в которой имеется актуальный веб-браузер.

Всего предусмотрено шесть видов концептов, из которых пять используются в НСКК: угрозы, ресурсы, промежуточные концепты, цели и контрмеры, которые для удобства и наглядности различаются цветами.

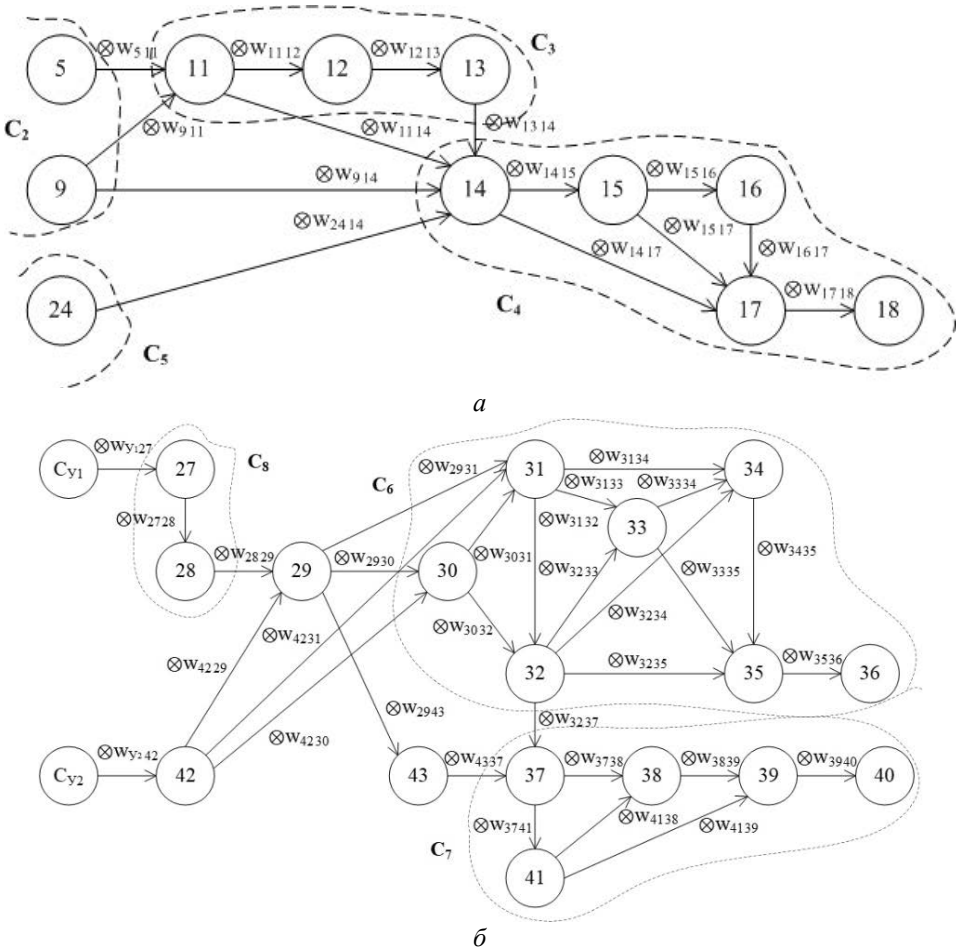

Рис. 5. Декомпозиция концептов: $а$ – C_3, C_4; $б$ – C_6, C_7 и C_8 исходной НСКК для оценки рисков АИС

Набор опций зависит от типа концепта, но в большинстве случаев задается его название с описанием, а также текущее состояние. В случае когда веса всех связей, указывающих на концепт, предполагаются одинаковыми, можно отметить опцию «Навязанный вес» и задать нужное значение. Для контрмер допустимо указать, копией какой существующей контрмеры она является, что позволяет реализовывать ситуации, когда одна контрмера воздействует сразу на несколько связей.

Для установления связей между концептами необходимо нажать на кнопку «Размещение» группы действий «Связи» в окне инструментов. После этого связи размещаются путем нажатия последовательно на начальный и конечный элемент. Размещенные контрмеры и начальные состояния концептов можно регулировать и комбинировать, создавая различные сценарии, которые позволяют сравнивать эффективность контрмер.

На рис. 6 приведен пример НСКК оценки рисков, построенной в «Cognitive Map Constructor».

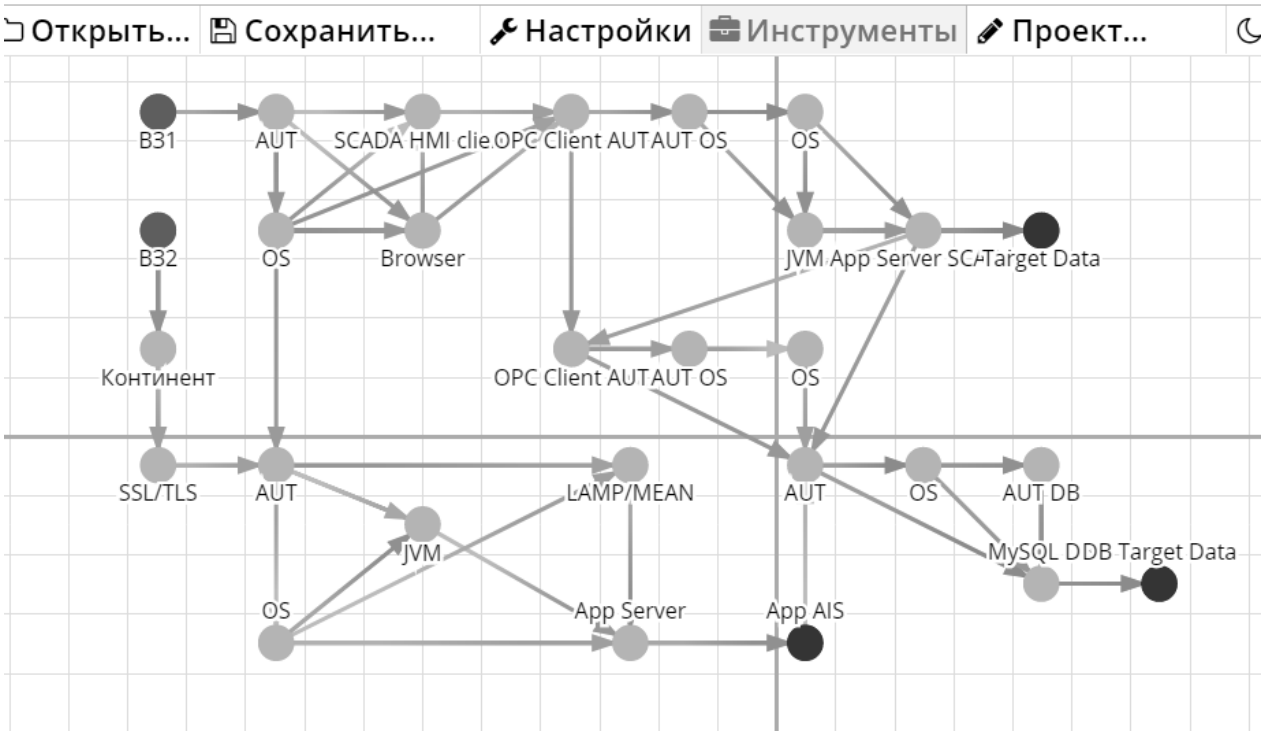

Рис. 6. НСКК для оценки рисков подсистемы сбора и хранения данных на станциях обслуживания (Зона 1)

Можно увидеть, как изменяются состояния концептов во времени («Состояния» в подменю «Проект…»), и узнать, какое состояние у целевых концептов НСКК (рис. 7).

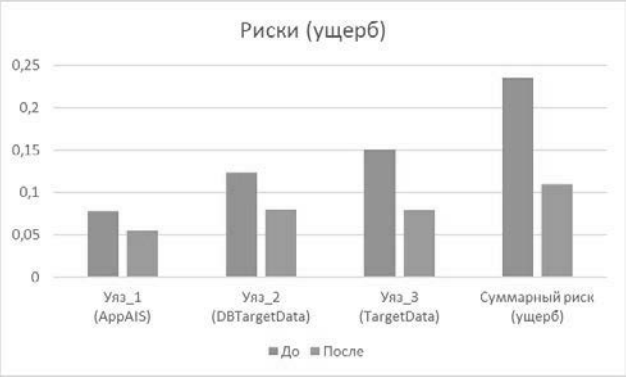

Рис. 7. Оценка рисков для целевых концептов и оценка суммарного риска до и после реализации контрмер. По оси ординат оценка условного риска

Здесь AppAIS – Эксплуатация уязвимости Web-приложения для запуска модуля доступа к БД оперативного хранения ТМИ на станциях обслуживания ЛА; DB Target Data – модификация оперативных данных ТМИ в БД хранения; Target Data – модификация ТМИ в долгосрочном хранилище.

ЗАКЛЮЧЕНИЕ

Перспективным способом решения задачи оценки рисков обеспечения целостности ТМИ является моделирование сценариев реализации угроз с помощью инструментов топологического анализа защищенности системы и когнитивного моделирования с применением нечетких серых когнитивных карт.

В основе данного подхода может использоваться построение исходной НСКК для оценки рисков АИС с последующей декомпозицией НСКК на ряд вложенных когнитивных карт следующих уровней детализации (аналогично тому, как это делается в технологии функционального моделирования IDEF0). Особенности построения данной процедуры рассмотрены в статье применительно к задаче обеспечения целостности ТМИ в системе сбора, хранения и обработки информации о состоянии бортовых систем ЛА. Показано, что использование НСКК позволяет получить количественные оценки факторов риска с учетом возможного разброса фактически располагаемых данных и мнений экспертов.

Для автоматизации предложенной процедуры оценки рисков с использованием НСКК разработано программное средство «Cognitive Map Constructor», с помощью которого можно выявить наиболее опасные уязвимости в исследуемой АИС, а также оценить эффективность реализации различных мероприятий (контрмер) по защите ТМИ от воздействия внешних и внутренних угроз.

СПИСОК ЛИТЕРАТУРЫ

1. **Ландшафт** угроз для систем промышленной автоматизации. Второе полугодие 2018. [Электронный ресурс]. URL: https://ics-cert.kaspersky.ru/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/ (дата обращения 17.08.2019). **[** *Threat landscape for industrial automation systems. H2 2018,* (2019, Aug. 17). [Online]. Available: https://ics-cert.kaspersky.com/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/ **]**

2. **Кибербезопасность** – 2018-2019: итоги и прогнозы [Positive Technologies Research]. [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2018-2019/ (дата обращения 17.08.2019). **[** *Cybersecurity - 2018-2019: results and forecasts [Positive Technologies Research],* (2019, Aug. 17). [Online]. Available: https://www.ptsecurity.com/ru-ru/research/analytics/ cybersecurity-2018-2019/ **]**

3. **Ярушевский Д.** Кибербезопасность АСУ ТП – что это и зачем? // Пресс-центр «ДиалогНаука». [Электронный ресурс]. URL: https://www.dialognauka.ru/press-center/article/13226/ (дата обращения 17.08.2019). **[** D. Yarushevskij (2019, Aug. 17), "ICS cybersecurity - what is it and why?", (in Russian), *in Press-centr "DialogNauka"* [Online]. Available: https://www.dialognauka.ru/press-center/article/13226/ **]**

4. **Васильев В. И., Кириллова А. Д., Кухарев С. Н.** Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) // Вестник УрФО. Безопасность в информационной сфере. 2018. № 4 (30). С. 66–74. **[** V. I. Vasilyev, A. D. Kirillova, S. N. Kukharev, "Cybersecurity of APCS: modern trends and approaches (current state, perspectives)", (in Russian), in *Vestnik UrFO. Bezopasnost' v informacionnoj sfere*, no. 4 (30), pp. 66-74, 2018. **]**

5. **Информационная** безопасность автоматизированных систем управления технологическими процессами / Ю. С. Андреев и др. // Известия вузов. Приборостроение. 2019. Т. 62, № 4. С. 331–339. **[** U. S. Andreev, et al., "Information Security of Automated Process Control Systems", (in Russian), in *Izvestiya vuzov. Priborostroenie*, vol. 62, No. 4, pp. 331-339, 2019. **]**

6. **Астахов А. М.** Искусство управления информационными рисками. М.: ДМК Пресс. 2010. 312 с. **[** A. M. Astahov, *The art of information risk management*, (in Russian). Moscow: DMK Press, 2010. **]**

7. **Аникин И. В.** Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях. Казань: Ред.-изд. Центр «Школа», 2015. 224 с. **[** I. V. Anikin, *Methods for assessing and managing information security risks in corporate information networks*, (in Russian). Kazan': Red.-izd. Centr «Shkola», 2015. **]**

8. **Ажмухамедов И. М.** Анализ и управление комплексной безопасностью на основе когнитивного моделирования // Управление большими системами: сборник трудов. 2010. №. 29. С. 5−15. **[** I. M. Azmuhamedov, "Cognitive-modeling-based integrated security analysis and management", (in Russian), in *Upravlenie bol'shimi sistemami: sbornik trudov*, no. 29, pp. 5-15, 2010. **]**

9. **Yeboah-Boateng E. O.** Using Fuzzy Cognitive Maps (FCMs) to Evaluate the Vulnerabilities with ICT Assets Disposal Policies // Intern. Journal on Electrical & Computer Sciences IJECS-IJENS. Oct. 2012. Vol. 12, No. 05. Pp. 20-31. **[** E. O. Yeboah-Boateng, "Using Fuzzy Cognitive Maps (FCMs) to Evaluate the Vulnerabili-ties with ICT Assets Disposal Policies", in *Intern. Journal on Electrical & Computer Sciences IJECS-IJENS.*, vol. 12, no. 05, pp. 20-31, 2012. **]**

10. **Szwed P., Skrzynski P. A.** New Lightweight method for security risk assessment based on Fuzzy Cognitive Maps // Intern. Journal on Appl. Math. Comput. Sci. 2014. Vol. 24, No. 1. Pp. 213-225. **[** P. Szwed, P. A. Skrzynski, "New Lightweight method for security risk assessment based on Fuzzy Cognitive Maps", in *Intern. Journal on Appl. Math. Comput. Sci.*, vol. 24, no. 1, pp. 213-225, 2014. **]**

11. **Васильев В. И., Вульфин А. М., Гузаиров М. Б.** Оценка рисков информационной безопасности с использованием нечетких продукционных когнитивных карт // Информационные технологии. 2018. Т. 24, № 4. С. 266–273. **[** V. I. Vasilyev, A. M. Vulfin, M. B. Guzairov, "Information security risk assessment using fuzzy production cognitive maps", (in Russian), in *Informacionnye tekhnologii*, vol. 24, no. 4, pp. 266-273, 2018. **]**

12. **Salmeron J. L.** Modelling grey uncertainty with Fuzzy Grey Cognitive Maps // Expert Systems with Applications. 2010. Vol. 37, No. 12. Pp. 7581-7588. **[** J. L. Salmeron, "Modelling grey uncertainty with fuzzy grey cognitive maps", in *Expert Systems with Applications*, vol. 37, no. 12, pp 7581-7588, 2010. **]**

13. **Интервальное** оценивание информационных рисков с помощью нечетких серых когнитивных карт / В. И. Васильев и др. // Информационные технологии. 2018. Т. 24, № 10. С. 657–664. **[** V I. Vasilyev, et al, "Interval estimation of information risks with use of Fuzzy Grey Cognitive Maps", (in Russian), in *Informacionnye tehnologii*, vol. 24, no. 10, pp. 657-664, 2018. **]**

14. **Architecture** of the security access system for information on the state of automatic control systems of aircraft / A. I. Frid, et. al. // Proceedings of the 19th International Workshop on Computer Science and Information Technologies CSIT'2017, (Germany, Baden-Baden, October 8-10, 2017). Vol. 2. Pp. 21-27. **[** A. I. Frid, et. al., "Architecture of the security access system for information on the state of automatic control systems of aircraft", in *Proceedings of the 19th International Workshop on Computer Science and Information Technologies* (CSIT'2017), vol. 2, pp. 21-27, 2017. **]**

15. **Анализ** защищенности системы сбора, хранения и обработки телеметрической информации о состоянии бортовых систем летательного аппарата / М. Б. Гузаиров и др. // Вестник УГАТУ 2019 (в настоящем выпуске). **[** M B. Guzairov, et al., "Analysis of system protection under collection, storage and processing of telemetric information on the condition of flying vehicle", (in Russian), in *Vestnik UGATU*, 2019. **]**

16. **Бельский С. М.** Cognitive Map Constructor // Свидетельство о гос. регистрации программы для ЭВМ № 2019614381 от 03.04.2019 **[** S. M. Belsky, "Cognitive Map Constructor", Computer Program no. 2019614381, 2019. **]**

ОБ АВТОРАХ

ВАСИЛЬЕВ Владимир Иванович, проф. каф. ВТиЗИ УГАТУ. Дипл. инж. по пром. электронике (УАИ, 1970). Д-р техн. наук по сист. анализу и автоматич. управлению (ЦИАМ, 1990). Иссл. в обл. интеллектуальных систем управления и защиты информации.

ВУЛЬФИН Алексей Михайлович, доц. каф. ВТиЗИ УГАТУ. Дипл. инж.-программиста (УГНТУ, 2008). Канд. техн. наук по системному анализу, управлению и обработке информации (УГАТУ, 2012). Иссл. в обл. интеллектуального анализа данных и моделирования сложных технических систем.

БЕРХОЛЬЦ Виктория Викторовна, асп. каф. ВТиЗИ УГАТУ. Дипл. инженера по специальности: вычислительные машины, комплексы, системы и сети (УГАТУ, 2015). Иссл. в обл. обеспечения информационной безопасности.

КИРИЛЛОВА Анастасия Дмитриевна, асп. каф. ВТиЗИ УГАТУ. Дипл. магистра по направлению: информатика и вычислительная техника (УГАТУ, 2017). Иссл. в обл. обеспечения информационной безопасности.

БЕЛЬСКИЙ Станислав Михайлович, студент каф. ВТиЗИ УГАТУ.

METADATA

Title: Risk analysis for ensuring the integrity of telemetric information using cognitive modeling technology

Authors: V. I. Vasilyev [1], A. M. Vulfin [2], V. V. Berkholts [3], A. D. Kirillova [4], S. M. Belskii [5]

Affiliation:

Ufa State Aviation Technical University (UGATU), Russia.

Email: [1] vasilyev@ugatu.ac.ru, [2] vulfin.alexey@gmail.com, [3] torina4@yandex.ru, [4] kirillova.andm@gmail.com, [5] 1902199615@mail.ru

Language: Russian.

Source: Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), vol. 23, no. 4 (86), pp. 122-131, 2019. ISSN 2225-2789 (Online), ISSN 1992-6502 (Print).

Abstract: The issues of risk analysis of information security of telemetric information on the state of the onboard subsystems of the aircraft are considered. A method for assessing the risk of a system for collecting, storing and processing telemetric information based on cognitive modeling technology using fuzzy gray cognitive maps is proposed. A software tool has been developed to automate the risk assessment process.

Key words: information security; risk assessment; information integrity; fuzzy gray cognitive map

About authors:

VASILYEV, Vladimir Ivanovich, Prof., Dept. of Computer Engineering and Information Security. Dipl. Engineer in Industrial Electronics (USATU, 1970), Dr. of Tech. Sci. (CIAM, 1990). Research. in intelligent systems of control and information security.

VULFIN, Alexey Mikhailovich, Ass.-prof., Dept. of computing equipment and information protection, software engineer dipl. (UGNTU, 2008). Cand. of tech. sci. in System Analysis, Management and Information Processing (USATU, 2012). Research in the region data mining and modeling of complex technical systems.

BERKHOLTS, Victoria Victorovna, Postgrad. Student, Dept. of Computer Engineering and Information Security. Dipl. Engineer's in Computers, complexes, systems and networks (USATU, 2017). Research in the area of information security.

KIRILLOVA, Anastasia Dmitriyevna, Postgrad. Student, Dept. of Computer Engineering and Information Security. Master's Degree of Informatics and Computing (USATU, 2017). Research in the area of information security.

BELSKII, Stanislav Mikhailovich, Student, Dept. of Computer Engineering and Information Security (USATU).