УДК 004.89 DOI: 10.17587/it.26.213-221

В. И. Васильев, д-р техн. наук, проф., e-mail: vasilyev@ugatu.ac.ru,
А. М. Вульфин, канд. техн. наук, доц., e-mail: vulfin.alexey@gmail.com,
М. Б. Гузаиров, д-р техн. наук, проф., e-mail: guzairov@ugatu.su,
В. М. Картак, д-р физ.-мат. наук, доц., e-mail: kvmail@mail.ru,
Л. Р. Черняховская, д-р техн. наук, проф., e-mail: lrchern@yandex.ru,
Уфимский государственный авиационный технический университет

Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт[1]

Рассмотрены методические аспекты количественной оценки рисков кибербезопасности АСУ ТП промышленных предприятий. В качестве базового подхода предлагается использование риск-ориентированного подхода, заложенного в основу стандартов серии ГОСТ Р 62443. Применение вложенных нечетких серых когнитивных карт при этом обеспечивает возможность получить более обоснованные и достоверные количественные оценки показателей рисков кибербезопасности АСУ ТП. Рассмотрен пример применения данной технологии для оценки защищенности телеметрической информации о состоянии бортовых авиационных систем.

Ключевые слова: *кибербезопасность, оценка рисков, когнитивное моделирование, нечеткая серая когнитивная карта*

Введение

В последние годы в нашу жизнь все более прочно входят новые термины и понятия: "цифровизация экономики", "промышленный интернет вещей", "киберфизические системы", "киберпространство", "кибербезопасность". Неизбежным следствием промышленной революции 4.0 при этом является не только ожидаемый рост эффективности, качества и производительности производства, но и все

[1]Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-00-00238 КОМФИ.

возрастающая зависимость от безопасности и надежности функционирования инфраструктуры промышленных систем автоматизации и контроля.

Согласно данным, приведенным в отчете "Лаборатории Касперского" [1], промышленные предприятия все чаще становятся мишенью и жертвами целевых кибератак (Advanced Persistent Threats, APT). По итогам 2018 г. общий процент атакованных АСУ ТП, на которых были обнаружены вредоносные объекты, вырос по сравнению с 2017 г. на 3,2 % и составил 47,2 %. В России в течение второго полугодия 2018 г. хотя бы один раз вредоносные объекты были зафиксированы на 45,3 % компьютеров АСУ. На сайте "Лаборатории Касперского" (US ICS-CERT) опубликовано 415 уязвимостей, выявленных в 2018 г. в различных компонентах АСУ ТП, что на 28,9 % превышает уровень 2017 г. Более половины выявленных в системах АСУ ТП уязвимостей получили при этом более 7 баллов по шкале CVSS версии 3.0, что соответствует высокой и критической степени риска.

Отметим еще одно важное обстоятельство, накладывающее свой отпечаток на задачи обеспечения безопасности АСУ ТП. Современные технологические сети предприятий находятся в тесном взаимодействии с многочисленными организациями-смежниками (подрядчики, разработчики, системные интеграторы, поставщики облачных решений и т.д.). Очевидно, что это открывает возможности подключения компьютеров сотрудников указанных организаций к технологической сети обслуживаемого предприятия извне (напрямую или удаленно через сеть Интернет) и может являться одним из каналов проникновения вредоносного ПО в технологические сети.

Задачи обеспечения кибербезопасности промышленных автоматизированных систем при этом принципиально отличаются от классических задач обеспечения информационной безопасности [2, 3]. С точки зрения кибербезопасности главным защищаемым ресурсом в АСУ ТП является сам технологический процесс, и основная цель — это обеспечить его непрерывность (т.е. доступность всех узлов) и целостность (в том числе передаваемой между узлами информации). В корпоративных информационно-вычислительных системах главный ресурс — это информация, которая обрабатывается, передается и хранится в системе, а основная цель — обеспечение ее конфиденциальности. Таким образом, поле потенциальных рисков и угроз для АСУ ТП по сравнению с корпоративными информационными системами расширяется за счет рисков потенциального ущерба жизни и здоровью персонала, населения и окружающей среде.

Отсюда понятен особый интерес к решению проблемы обеспечения кибербезопасности АСУ ТП, включая создание нормативно-правовой и методической базы (краткую характеристику современного состояния и полученных результатов в этой области можно найти в работе [4]). Одним из перспективных путей решения данной проблемы является разработка и поэтапное принятие серии международных стандартов ISA/IEC 62443 [5]. Всего в этой серии запланирован выпуск 13 руководящих документов, три из которых уже переведены на русский язык и утверждены в России (ГОСТ Р 62443). В основе развиваемого в этих стандартах риск-ориентированного подхода используется методология формирования требований по обеспечению кибербезопасности АСУ ТП в зависимости от уровня рисков предприятия подвергнуться кибератакам. В стандартах подчеркивается необходимость применения для этих целей не только критериев качественной оценки уровня безопасности АСУ ТП, но и разработки количественных методов оценки безопасности на основе математических моделей риска, угроз и инцидентов безопасности.

Рассмотрению одного из возможных подходов к решению данной задачи с использованием технологии когнитивного моделирования (и, в частности, математического аппарата "вложенных" нечетких серых когнитивных карт) посвящена данная статья.

1. Нечеткие когнитивные карты и принцип вложения

Технологии когнитивного моделирования, основанные на построении нечетких когнитивных карт, сегодня успешно используются при изучении поведения сложных социально-экономических и организационно-технических систем. Преимуществами нечетких когнитивных карт (Fuzzy Cognitive Maps, FCM), предложенных в 1986 г. Б. Коско [6], являются их наглядность, возможность выявления структуры причинно-следственных связей между элементами сложной системы, трудно поддающейся количественному анализу традиционными методами, использование знаний и опыта экспертов в исследуемой предметной области. Известны примеры применения нечетких когнитивных

карт при решении задач оценки рисков информационной безопасности [7—12].

Вместе с тем, на практике изучение реального сложного объекта (системы, проблемы) с помощью нечеткого когнитивного моделирования встречается с рядом труднопреодолимых факторов (высокая размерность пространства состояний исследуемой системы, неоднозначность выбора состава концептов и выявления наиболее существенных (значимых) связей между ними, неопределенность в оценке силы этих связей и т.д. — т.е. все то, что составляет "проклятие размерности"). Попытки разрешить эту ситуацию, как правило, связаны с представлением исходной нечеткой когнитивной карты (НКК) системы в виде совокупности из нескольких, более простых с точки зрения анализа, НКК, взаимодействующих между собой по вертикали или по горизонтали. В качестве инструмента для исследования сложных систем сегодня эффективно применяются такие модификации НКК, как иерархические НКК [13], многоагентные НКК [14], многослойные (вложенные) НКК [15—17].

Отметим, что в отличие от иерархических и многоагентных НКК основной упор при построении вложенных НКК (Nested FCM) делается на последовательном раскрытии неопределенностей — каждый последующий (нижележащий) слой содержит более детальную (локальную) информацию о внутренней структуре (топологии) базовых концептов исходной НКК. Ниже нами будет рассматриваться именно этот класс нечетких когнитивных моделей, в основе которых используется принцип вложения (nesting principle).

В качестве базового подхода к построению вложенных НКК можно воспользоваться предложенной в работе [18] теорией декомпозиции больших НКК. Согласно этой теории процедура когнитивного моделирования начинается с построения подробной (развернутой) НКК исследуемой системы, которая принимается в качестве исходной. Затем проводится разбиение множества вершин (концептов) данной НКК на ряд отдельных блоков в соответствии с отношением эквивалентности. Каждый из этих блоков содержит локальную информацию о взаимодействиях и внутренних зависимостях между концептами в пределах данного блока. Рассматривая полученные блоки в качестве вершин укрупненной (обобщенной) НКК (которую авторы [18] назвали Quotient Fuzzy Cognitive Map), получим новое блочное представление НКК.

На рис. 1 показан пример подобной декомпозиции НКК (слева — исходная НКК, состоящая из шести индивидуальных блоков (частных НКК), определенным образом связанных между собой; справа — укрупненная НКК, каждая из вершин (концептов) которой отражает множество вершин (концептов) соответствующей частной НКК.

Заметим, что в отличие от описанной выше процедуры преобразования НКК [18] путем ее "сворачивания" (т.е. от частного к общему) мы ниже, наоборот, будем строить вложенную НКК путем ее "развертывания", детализации (от общего к частному). Будем полагать, что рассматриваемая вложенная НКК строится в классе нечетких серых когнитивных карт (Fuzzy Grey Cognitive Maps, FGCM), предложенных в 2010 г. Хосе Салмероном [19]. Основное отличие нечетких серых когнитивных карт (НСКК) от других классов НКК — использование интервальных значений переменных состояния концептов и весов связей между концептами вместо нечетких чисел или термов лингвистических переменных, как это традиционно делается в НКК. Считается, что НСКК лучше соответствуют представлениям экспертов, обладают большей интерпретируемостью и предоставляют больше степеней свободы лицу, принимающему решение (ЛПР), по результатам моделирования.

Согласно работе [19] НСКК — это когнитивная модель системы в виде ориентированного графа, заданного с помощью следующей тройки множеств:

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

где $C = \{C_i\}$ — множество концептов (вершин графа), $i = 1, 2, ..., n$; $F = \{F_{ij}\}$ — множество связей между концептами (дуг графа); $W = \{W_{ij}\}$ — множество отношений межу концептами, задан-

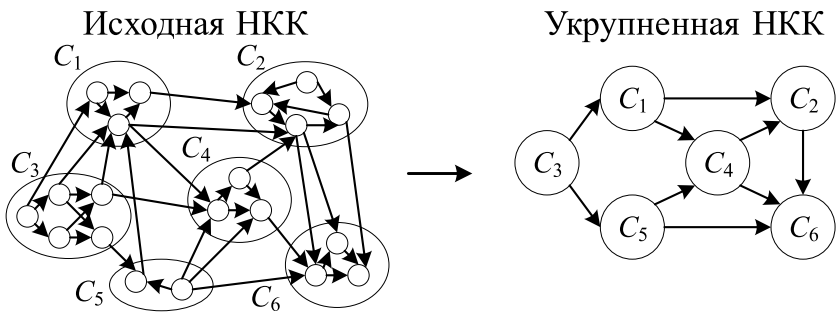

Рис. 1. Пример декомпозиции НКК

ных в виде весов соответствующих связей (дуг графа), $(i, j) \in \Omega$. Здесь $\Omega = \{(i_1, i_2), ..., (i_L, j_L)\}$ — множество индексов вершин, связанных между собой; L — число связей (дуг графа), $L \leqslant n(n-1)$.

В отличие от традиционного способа задания НКК, веса связей НСКК задаются с помощью "серых" (интервальных) чисел, которые обозначаются $\otimes W_{ij}$ и определяются следующим образом:

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

где $\underline{W}_{ij} < \overline{W}_{ij}$; $[\underline{W}_{ij}, \overline{W}_{ij}] \in [-1, 1]$; $\underline{W}_{ij}, \overline{W}_{ij}$ — соответственно нижняя и верхняя границы серого числа $\otimes W_{ij}$. В частном случае, когда $\underline{W}_{ij} = \overline{W}_{ij}$, получаем $\otimes W_{ij} \in [\underline{W}_{ij}, \underline{W}_{ij}]$ — "белое" (обычное) число.

Изменение состояния концептов во времени при этом описывается уравнениями

$$\otimes X_i(k+1) = f\left(\otimes X_i(k) + \sum_{\substack{j=1 \\ (j \neq i)}}^{n} \otimes W_{ji} \otimes X_j(k)\right), \qquad (3)$$

$i = 1, 2, \ldots, n,$

где $\otimes X_i(k)$ — "серая" (интервальная) переменная состояния i-го концепта НСКК, в каждый момент времени $k = 0, 1, 2, ...$ принимающая значение внутри некоторого интервала $[\underline{X}_i(k), \overline{X}_i(k)]$ из интервала $[-1, 1]$; $f(\cdot)$ — нелинейная функция активации i-го концепта, отображающая значения аргумента в интервал $[-1, 1]$. Для определенности будем полагать, что в качестве функции активации принимается двухполярная сигмоида (гиперболический тангенс):

$$f(x) = (1 - \mathbf{e}^{-x})/(1 + \mathbf{e}^{-x}) = \mathrm{th}(x/2). \qquad (4)$$

Для решения уравнений (3) необходимо задать начальные условия для переменных состояния $\otimes X_i(0)$, которые также представляют собой серые числа $\otimes X_i(0) \in [\underline{X}_i(0), \overline{X}_i(0)]$, $i = 1, 2, \ldots, n$.

2. Методика анализа рисков с помощью нечетких серых когнитивных карт

Рассмотрим методику анализа рисков обеспечения кибербезопасности АСУ ТП с использованием вложенных нечетких когнитивных карт на следующем примере. В качестве объекта защиты будем рассматривать автоматизированную информационную систему (АИС) сбора, хранения и обработки телеметрической информации (ТМИ) предприятия-изготовителя изделий авиационной техники. Текущая информация о параметрах состояния бортовых систем собирается в течение всего периода их эксплуатации наземными службами технического обслуживания. Детальный анализ этой информации позволяет в последующем принимать правильные управленческие и конструкторские решения о дальнейшей эксплуатации и модификации бортовых систем летательного аппарата. Поэтому задача обеспечения целостности ТМИ в условиях воздействия на нее внешних и внутренних угроз имеет важное значение.

Обобщенная структура перспективной территориально распределенной АИС сбора, хранения и обработки ТМИ на станциях технического обслуживания приведена на рис. 2 (см. вторую сторону обложки).

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

1) *подсистема сбора и хранения первичных данных на станциях технического обслуживания* (зона 1), в состав которой входят:

- 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 предприятия-изготовителя (ПИ) авиационной техники;

2) *ядро корпоративной информационной сети (КИС)* ПИ (зона 2), где

- элемент 6 — клиентская часть для организации доступа к серверу станции обслуживания в целях передачи накопленных оперативных данных ТМИ в хранилище ПИ;
- элемент 8 — АРМ администратора и обслуживающего персонала ядра КИС ПИ;

3) *подсистема хранения ТМИ с функциями обеспечения отказоустойчивости* (зона 3), где:

- элемент 7 — узел доступа к хранилищу данных ТМИ на ПИ;
- Cluster management server — сервер управления вычислительным кластером и консоль управления системой мониторинга целостности;
- Core switch — базовый коммутатор вычислительного кластера;

4) *подсистема обработки данных ТМИ с помощью иерархии математических моделей* изделий авиационной техники (зона 4);

5) *подсистема поддержки и реализации бизнес-процессов ПИ* (зона 5).

Соответствующие подсистемы (зоны безопасности) связаны между собой на рис. 2 (см. вторую сторону обложки) с помощью каналов телекоммуникаций (трактов).

Используя в качестве инструмента моделирования аппарат НСКК, обратимся к задаче анализа рисков, связанных с обеспечением целостности ТМИ в рассмотренной выше АИС с учетом воздействия на систему внешних и внутренних угроз. Укрупненная НСКК для оценки рисков АИС, выступающая в данном случае как когнитивная модель АИС начального приближения (нулевой уровень декомпозиции), представлена на рис. 3.

Здесь используются следующие обозначения: верхний индекс (маркер "*") обозначает принадлежность концепта C_p^* укрупненной НСКК, нижний индекс p обозначает номер концепта текущего уровня.

Выбор серых значений весов связей $\otimes W_{ij}$ для НСКК на рис. 3 должен проводиться экспертом с учетом его опыта и субъективных оценок вероятностей использования уязвимостей АИС (табл. 1), что на практике весьма затруднительно. Учитывая, что каждое из указанных событий представляет собой сложное событие, состоящее из цепочки следующих друг за другом элементарных событий, целесообразно декомпозировать изображенную на рис. 3 НСКК, представив ее в виде набора вложенных НСКК для отдельных концептов (т.е. зон безопасности, содержащих целевые объекты атаки на ТМИ через соответствующие уязвимости АИС).

Первый уровень декомпозиции исходной (укрупненной) НСКК представлен на рис. 4

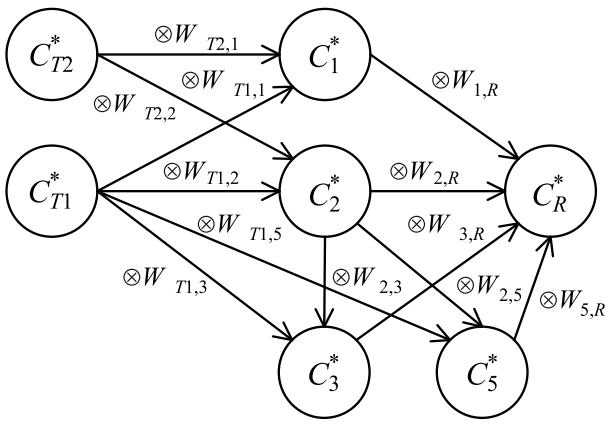

Рис. 3. Укрупненная (исходная) НСКК для оценки рисков АИС

Таблица 1

Список концептов укрупненной НСКК

Концепт	Наименование концепта
$C^*_{T_1}$	Внутренняя угроза целостности ТМИ (вследствие сбоев или ошибочных действий персонала)
$C^*_{T_2}$	Внешняя угроза целостности ТМИ (вследствие попытки несанкционированного доступа извне к информации)
C^*_1	Модификация данных ТМИ в Зоне 1
C^*_2	Модификация данных ТМИ в Зоне 2
C^*_3	Модификация данных ТМИ в Зоне 3
C^*_5	Модификация данных ТМИ в Зоне 5
C^*_R	Риск (потенциальный ущерб), вызванный нарушением целостности ТМИ в АИС

(см. третью сторону обложки). Здесь используются следующие обозначения: верхний индекс q концепта C_p^q указывает на его принадлежность к концепту C_q^* укрупненной НСКК; нижний индекс p — номер концепта в НСКК первого уровня декомпозиции. Список концептов первого уровня декомпозиции НСКК приведен в табл. 2.

На рис. 5 представлен второй уровень декомпозиции для концепта C_1^*, позволяющий уточнить воздействие угроз на рассматриваемый концепт.

На схеме используются следующие обозначения концептов $C_r^{q,p}$ второго уровня декомпозиции НСКК: верхний индекс q — номер концепта (родительский концепт нулевого уровня декомпозиции) укрупненной НСКК, в состав которого входит данный элемент; индекс p — номер родительского концепта первого уровня декомпозиции; нижний индекс r — номер концепта текущего уровня. Список концептов второго уровня декомпозиции НСКК для зоны 1 приведен в табл. 3.

Дальнейшая декомпозиция второго уровня позволяет перейти к еще более детальной НСКК, позволяющей учитывать влияние отдельных уязвимостей на потенциальное нарушение целостности ТМИ в промежуточных элементах обработки информации.

Рассмотрим численный пример оценки рисков для концепта C_1^* (рис. 5). Будем полагать, что при выборе серых значений весов НСКК необходимо ориентироваться на некоторую нечеткую шкалу, определяющую силу связей между собой различных концептов (табл. 4).

Допустим далее, что эксперт оценил значения весов связей НСКК на рис. 5 (табл. 5).

Таблица 2

Список концептов первого уровня декомпозиции НСКК

Концепт	Наименование концепта	Родительский концепт
$T_1^1, \ldots, T_1^8$	Внутренние угрозы целостности ТМИ (т.е. точки потенциальной реализации угрозы нарушения целостности ТМИ внутренним субъектом)	T_1^*
T_2^1, T_2^2	Внешние угрозы целостности ТМИ (декомпозиция концепта T_2^*)	T_2^*
C_1^1	Доступ к данным ТМИ в клиент-серверной SCADA web-base до внесения в БД оперативного хранилища ТМИ	C_1^* (Зона 1)
C_2^1	Доступ к БД оперативного хранения данных ТМИ	
C_3^1	Доступ к сетевому оборудованию	
C_4^1	Доступ к модулю Web-сервера отправки данных ТМИ в долгосрочное хранилище ПИ	
C_5^2	Доступ к сетевой инфраструктуре	C_2^* (Зона 2)
C_6^2	Доступ к модулю Web-клиента, реализующего прием ТМИ на ПИ с удаленных станций обслуживания	
C_8^2	Несанкционированный доступ к рабочей станции ядра КИС ПИ	
C_{10}^2	Доступ к серверу отчетов о состоянии оборудования, формируемых для пользователей Зоны 4	
C_7^3	Получение доступа к ТМИ в долгосрочном хранилище	C_3^* (Зона 3)
C_9^5	Доступ к серверу управления вычислительным кластером Зоны 5	C_5^* (Зона 5)
IST^5	Модуль контроля целостности ТМИ	

Таблица 3

Список концептов второго уровня декомпозиции НСКК для зоны 1

Концепт	Наименование концепта	Родительский концепт
$C_1^{1,1}$	Доступ к HMI client SCADA	C_1^1
$C_2^{1,1}$	Доступ к оперативным данным ТМИ на client-server части SCADA до внесения в оперативное хранилище	
$C_3^{1,2}$	Доступ к клиенту для взаимодействия с сервером OPC UA	C_2^1
$C_4^{1,2}$	Доступ к БД хранения оперативных данных ТМИ	

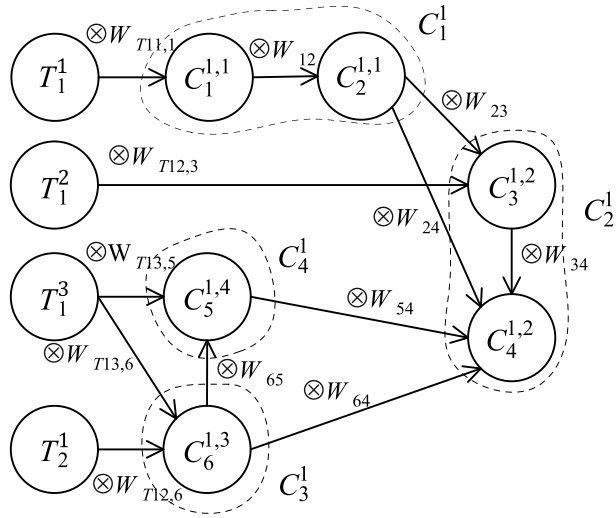

Рис. 5. Второй уровень декомпозиции НСКК для оценки рисков АИС в зоне 1

Таблица 4

Оценка силы связи между концептами

Лингвистическое значение силы связи	Числовой диапазон
Не влияет	0
Очень слабая	(0; 0,15]
Слабая	(0,15; 0,35]
Средняя	(0,35; 0,6]
Сильная	(0,6; 0,85]
Очень сильная	(0,85; 1]

Таблица 5

Значения весов связей НСКК

Вес связи	Значение веса связи	Серость (разброс оценки)
$\otimes W_{T11,1}$	[0,6; 0,75]	0,075
$\otimes W_{T12,3}$	[0,5; 0,7]	0,1
$\otimes W_{T13,5}$	[0,5; 0,7]	0,1
$\otimes W_{T13,6}$	[0,15; 0,3]	0,075
$\otimes W_{T21,6}$	[0,55; 0,65]	0,05
$\otimes W_{12}$	[0,35; 0,55]	0,1
$\otimes W_{23}$	[0,55; 0,65]	0,05
$\otimes W_{24}$	[0,3; 0,5]	0,1
$\otimes W_{34}$	[0,15; 0,3]	0,075
$\otimes W_{54}$	[0,2; 0,45]	0,125
$\otimes W_{64}$	[0,24; 0,35]	0,055
$\otimes W_{65}$	[0,22; 0,37]	0,075

Используя для расчетов программное средство "Cognitive Map Constructor" (см. раздел 3 настоящей статьи), выполним оценку изменения верхней и нижней границ переменной состояния концептов НСКК во времени $k = 1, 2, 3, ...$ (табл. 6, 7). Состояния входных концептов T_1^1, T_1^2, T_1^3, T_2^1 при этом были заданы как [0,8; 1] для всех $k = 0, 1, 2, ...$; начальные условия для переменных состояния других концептов приняты нулевыми, т.е. равны [0; 0].

В результате установившееся значение серого вектора состояния $\otimes X$ для НСКК на рис. 5 (т.е. для декомпозиции концепта C_1^*) находится как

$$\otimes X = \{[0,42;0,58],[0,14;0,30],[0,42;0,65],$$
$$[0,36;0,71],[0,36;0,56],[0,48;0,67]\},$$

а искомое значение для состояния целевого концепта $C_4^{1,2}$ определяется серым числом [0,36; 0,71].

Рассмотрим состояние целевого концепта C_R^* (см. рис. 3), т.е. ущерба, вызванного потенциальным нарушением целостности ТМИ в АИС, после уточнения значений всех весовых коэффициентов по уровням декомпозиции исходной НСКК. Предположим, что активной является внутренняя угроза T_1^* нарушения целостности ТМИ, уровень которой определяется серым числом $\otimes X_{T_1}^* \in [0,6;0,95]$. Тогда получаем установившееся значение для оценки рисков вследствие нарушения целостности информации ТМИ: $\otimes X_R^* \in [0,19;0,28]$.

Допустим далее, что в качестве возможной контрмеры для снижения ущерба от нарушения целостности ТМИ применяется дополнительная система мониторинга, развернутая в виде защищенного контейнера в зоне 5. На рис. 4 данная система обозначена как модуль контроля целостности ТМИ — концепт IST^5. Защищенный контейнер обеспечивает мониторинг целостности ТМИ в режиме онлайн и офлайн путем анализа оперативных данных и данных, собранных в хранилище (зона 3).

Как показали расчеты, оценка рисков вследствие нарушения целостности информации ТМИ после применения дополнительной контрмеры составляет $\otimes X_R^*\big|_A \in [0,07;0,15]$, т.е. риск снижается в среднем в 2,3 раза.

Таблица 6

Верхние границы оценок состояния концептов

$\bar{X}_i$	k								
	1	2	3	4	5	6	7	8	9
$\bar{X}_1^{1,1}$	0,36	0,50	0,56	0,57	0,58	0,58	0,58	0,58	0,58
$\bar{X}_2^{1,1}$	0	0,10	0,19	0,24	0,27	0,29	0,29	0,30	0,30
$\bar{X}_3^{1,2}$	0,34	0,48	0,55	0,60	0,62	0,63	0,64	0,64	0,65
$\bar{X}_4^{1,2}$	0	0,10	0,19	0,26	0,31	0,33	0,35	0,36	0,36
$\bar{X}_5^{1,4}$	0,20	0,29	0,33	0,35	0,36	0,36	0,36	0,36	0,36
$\bar{X}_6^{1,3}$	0,27	0,39	0,44	0,46	0,47	0,47	0,48	0,48	0,48

Таблица 7

Нижние границы оценок состояния концептов

$\underline{X}_i$	k								
	1	2	3	4	5	6	7	8	9
$\underline{X}_1^{1,1}$	0,24	0,34	0,39	0,41	0,42	0,42	0,42	0,42	0,42
$\underline{X}_2^{1,1}$	0	0,04	0,08	0,11	0,13	0,13	0,14	0,14	0,14
$\underline{X}_3^{1,2}$	0,20	0,29	0,34	0,37	0,39	0,41	0,41	0,42	0,42
$\underline{X}_4^{1,2}$	0	0,28	0,51	0,63	0,68	0,70	0,71	0,71	0,71
$\underline{X}_5^{1,4}$	0,34	0,48	0,53	0,55	0,55	0,56	0,56	0,56	0,56
$\underline{X}_6^{1,3}$	0,44	0,60	0,65	0,66	0,67	0,67	0,67	0,67	0,67

3. Автоматизация процедуры анализа и управления рисками на основе технологии когнитивного моделирования

В целях повышения эффективности анализа и управления рисками с использованием НСКК было разработано специальное программное средство "Cognitive Map Constructor". Данное программное средство позволяет строить и редактировать НСКК, проводить с их помощью анализ рисков и обосновывать выбор необходимых контрмер из заданного пользователем набора. В результате строится диаграмма оценки рисков при различных сценариях внедрения контрмер и реализации угроз.

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 "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, а также способна работать на любой графической операционной системе, в которой имеется актуальный веб-браузер.

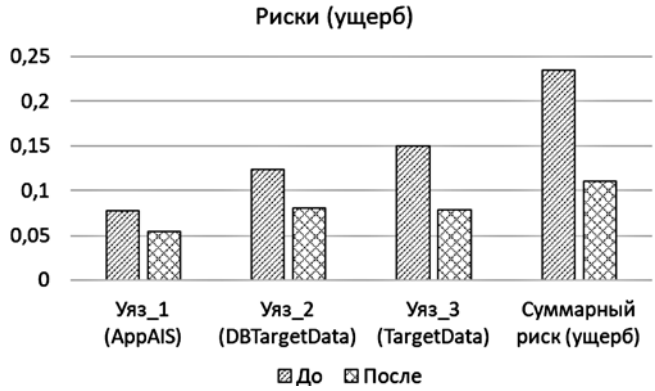

Рис. 7. Оценка рисков для целевых концептов и суммарного риска до и после реализации контрмер

На рис. 6 (см. третью сторону обложки) приведен пример НСКК оценки рисков подсистемы сбора и хранения данных АИС, построенной в "Cognitive Map Constructor".

Оценка рисков для целевых концептов и оценка суммарного риска до и после реализации контрмер и состояние целевых концептов НСКК приведены на рис. 7. Здесь: AppAIS — эксплуатация уязвимости Web-приложения для запуска модуля доступа к БД оперативного хранения ТМИ на станциях обслуживания ЛА; DBTargetData — модификация оперативных данных ТМИ в БД хранения; TargetData — модификация ТМИ в долгосрочном хранилище.

Заключение

Перспективным способом решения задачи оценки рисков кибербезопасности промышленных автоматизированных систем является моделирование сценариев реализации угроз с помощью когнитивного моделирования с применением нечетких серых когнитивных карт.

В основе данного подхода используется построение укрупненной НСКК для оценки рисков автоматизированной информационной системы, с последующей ее декомпозицией на ряд вложенных когнитивных карт следующих уровней детализации. Особенности построения данной процедуры рассмотрены на примере задачи обеспечения целостности ТМИ в промышленной автоматизированной системе сбора, хранения и обработки информации о состоянии авиационных бортовых систем. Использование НСКК позволяет при этом получить более достоверные оценки факторов риска с учетом возможного разброса фактически располагаемых данных и мнений экспертов.

Список литературы

1. **Ландшафт** угроз для систем промышленной автоматизации. Второе полугодие 2018. URL: https://ics-cert.kaspersky.ru/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/ (дата обращения 17.08.2019).

2. **Ярушевский Д.** Кибербезопасность АСУ ТП — что это и зачем? Пресс-центр "ДиалогНаука". URL: https://www.dialognauka.ru/press-center/article/13226/ (дата обращения 17.08.2019).

3. **Андреев Ю. С., Дергачев А. М., Жаров Ф. А., Садырин Д. С.** Информационная безопасность автоматизированных систем управления технологическими процессами // Известия вузов. Приборостроение. 2019. Т. 62, № 4. С. 331—339.

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.

5. **Ярушевский Д.** Обеспечение безопасности АСУ ТП — краткий обзор семейства стандартов IEC 62443 // Information Security/ Информационная безопасность. 2014. № 3. URL: http://lib.itsec.ru/articles2/ (дата обращения 17.08.2019).

6. **Kosko B.** Fuzzy Cognitive Maps // Intern. Journal of Man-Machine Studies. 1986. Vol. 1. P. 65—75.

7. **Гузаиров М. Б., Васильев В. И., Кудрявцева Р. Т.** Системный анализ информационных рисков с применением нечетких когнитивных карт // Инфокоммуникационные технологии. 2007. Т. 5, № 4. С. 42—48.

8. **Ажмухамедов И. М.** Динамическая нечеткая когнитивная модель влияния угроз на информационную безопасность системы // Безопасность информационных технологий. 2010. № 2. С. 68—72.

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, N. 05. P. 20—31.

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, N. 1. P. 213—225.

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.

12. **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.

13. **Stylios C. D., Groumpos P. P.** Fuzzy Cognitive Maps Multi-Model for Complex Manufacturing Systems // IFAC Large Scale Systems: Theory and Applications. Bucharest, Romania, 2001. P. 61—66.

14. **Stula M., Stipanicev D., Bodrozic L.** Intelligent Modeling with Agent-based Fuzzy Cognitive Map // Intern. Journal on Intell. Systems. 2010. Vol. 25, N. 10. P. 981—1004.

15. **Mohr S.** Modelling Approaches for Multilayer Fuzzy Cognitive Maps. URL: https://www.researchgate.net/publication/332158518_Modelling_Approaches_for_Multilayer_Fuzzy_Cognitive_Maps (дата обращения 17.08.2019).

16. **Mohagheghi S.** Fuzzy Cognitive Maps for Identifying Fault Activation Patterns in Automation Systems. URL: https://www.intechopen.com/books/ (дата обращения 17.08.2019).

17. **Motlagh O., Papageorgiou E. I., Tang S. H., Jamaludin Z.** Multivariate Relationship Modeling Using Nested Fuzzy Cognitive Map // Sains Malaysiana. 2014. N. 43(11). P. 1781—1790.

18. **Zhang J. Y., Liu Z. Q., Zhou S.** Quotient FCMs — A Decomposition Theory for Fuzzy Cognitive Maps // IEEE Transactions on Fuzzy Systems. Oct. 2003. Vol. 11, N. 5. P. 593— 604.

19. **Salmeron J. L.** Modelling grey uncertainty with Fuzzy Grey Cognitive Maps // Expert Systems with Applications. 2010. Vol. 37. N. 12. P. 7581—7588.

V. I. Vasilyev, Professor, e-mail: vasilyev@ugatu.ac.ru,
A. M. Vulfin, Associate Professor, e-mail: vulfin.alexey@gmail.com,
M. B. Guzairov, Professor, e-mail: guzairov@ugatu.su, **V. M. Kartak,** Professor, e-mail: kvmail@mail.ru,
L. R. Chernyakhovskaya, Professor, e-mail: lrchern@yandex.ru,
Ufa State Aviation Technical University, Ufa, 450077, Russian Federation

Cybersecurity Risk Assessment of Industrial Objects' ACS of TP on the Basis of Nested Fuzzy Cognitive Maps Technology

The paper is devoted to methodical aspects of quantitative assessment of cybersecurity risks for automated systems of control and checking the technological processes (ACS of TP) of modern industrial companies which are at present more often the objects of targeted attacks leading to widescale losses. As the basic approach to obtain the quantitative risk estimates, it is offered to use the system risk-oriented approach laid down in the series of international and national standards IEC 62443 and GOST R 62443. As the development of this approach, the authors offer the technique of ACS cybersecurity risks analysis consisting in formation on the basis of preliminary comprehensive examination of protected object its detailed cognitive model, reflecting the main factors leading to these risks, their interdependencies (cause-effect links) and final effects caused by these risks. The peculiarity of this cognitive model is its creation in the class of nested fuzzy grey cognitive maps, accumulating generally the information about both the global nature of risks character and the local mechanisms of their occurrence and propagation in the explored object. The application of mathematical apparatus of Fuzzy Grey Cognitive Maps (FGCM) here provides a possibility to obtain more reliable quantitative (interval) estimates of risks indices with account of disposable real statistical data. The example of using the offered technique of risks analysis for quantitative assessment of security level (integrity) of telemetric information used for monitoring and checking the parameters of onboard aviation systems condition at the stations of ground technical service is considered. The software tool "Cognitive Map Constructor" allowing to automate the main stages of applying this technique is developed.

Keywords: *cybersecurity, risk assessment, cognitive modeling, Fuzzy Grey Cognitive Map*

DOI: 10.17587/it.26...

References

1. **Threat landscape** for industrial automation systems. H2 2018, availible at: https://ics-cert.kaspersky.com/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/ (accessed 17 August 2019).

2. **Yarushevskij D.** ICS cybersecurity — what is it and why?, available at: https://www.dialognauka.ru/press-center/article/13226/ (accessed 17 August 2019) (in Russian).

3. **Andreev Yu. S., Dergachev A. M., Zharov F. A., Sadyrin D. S.** Information Security of Automated Process Control Systems, *Izvestiya Vuzov. Priborostroenie*, 2019. vol. 62, no. 4. pp. 331—339 (in Russian).

4. **Vasilyev V. I., Kirillova A. D., Kukharev S. N.** Cybersecurity of automated control systems of industrial objects: modern trends and approaches (current state, trends), *Vestnik UrFO. Bezopasnost' v Informacionnoj Sfere,* 2018, vol. 4(30), pp. 66—74 (in Russian).

5. **Yarushevskij D.** Security of ACS of TP — Overview of the IEC 62443 Family of Standards, *Information Security/Informacionnaya bezopasnost'*, 2014, no. 3, available at: http://lib.itsec.ru/articles2/ (accessed 17 August 2019) (in Russian).

6. **Kosko B.** Fuzzy Cognitive Maps, *Intern. Journal of Man-Machine Studies*, 1986, vol. 1, pp. 65—75.

7. **Guzairov M. B., Vasilyev V. I., Kudryavtseva R. T.** The system analysis of information risks with application of fuzzy cognitive maps, *Infokommunikatsionnye Tekhnologii*, 2007, vol. 5, no. 4, pp. 42—48 (in Russian).

8. **Azhmuhamedov I. M.** Dynamic fuzzy cognitive model of the threat influence on information security of the system, *Bezopasnost' Informacionnyh Tekhnologij.* 2010, no. 2, pp. 68—72 (in Russian).

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. 5, pp. 20—31.

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.

11. **Vasilyev V. I., Vulfin A. M., Guzairov M. B.** Information security risk assessment using fuzzy production cognitive maps, *Informatcionnye Tekhnologii.* 2018, vol. 24, no. 4, pp. 266—273 (in Russian).

12. **Vasilyev V. I., Vulfin A. M., Guzairov M. B., Kirillova A. D.** Interval estimation of information risks with use of Fuzzy Grey Cognitive Maps*, Informatcionnye Tehnologii*, 2018, 10(24), pp. 657—664 (in Russian).

13. **Stylios C. D., Groumpos P. P.** Fuzzy Cognitive Maps Multi-Model for Complex Manufacturing Systems, *IFAC Large Scale Systems: Theory and Applications.* Bucharest, Romania, 2001, pp. 61—66.

14. **Stula M., Stipanicev D., Bodrozic L.** Intelligent Modeling with Agent-based Fuzzy Cognitive Map, *Intern. Journal on Intell. Systems.* 2010, 25(10), pp. 981—1004.

15. **Mohr S.** Modelling Approaches for Multilayer Fuzzy Cognitive Maps, available at: https://www.researchgate.net/publication/332158518_Modelling_Approaches_for_Multilayer_Fuzzy_Cognitive_Maps (accessed 17 August 2019).

16. **Mohagheghi S.** Fuzzy Cognitive Maps for Identifying Fault Activation Patterns in Automation Systems, available at: https://www.intechopen.com/books/ (accessed 17 August 2019).

17. **Motlagh O., Papageorgiou E. I., Tang S. H., Jamaludin Z.** Multivariate Relationship Modeling Using Nested Fuzzy Cognitive Map, *Sains Malaysiana*. 2014, no. 43(11), pp. 1781—1790.

18. **Zhang J. Y., Liu Z. Q., Zhou S.** Quotient FCMs — A Decomposition Theory for Fuzzy Cognitive Maps, *IEEE Transactions on Fuzzy Systems.* Oct. 2003, vol. 11, no. 5, pp. 593— 604.

19. **Salmeron J. L.** Modelling grey uncertainty with Fuzzy Grey Cognitive Maps, *Expert Systems with Applications*, 2010, vol. 37, no. 12, pp. 7581—7588.

Рисунки к статье В. И. Васильева, А. М. Вульфина, М. Б. Гузаирова, В. М. Картака, Л. Р. Черняховской

«ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ АСУ ТП ПРОМЫШЛЕННЫХ ОБЪЕКТОВ НА ОСНОВЕ ВЛОЖЕННЫХ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ»

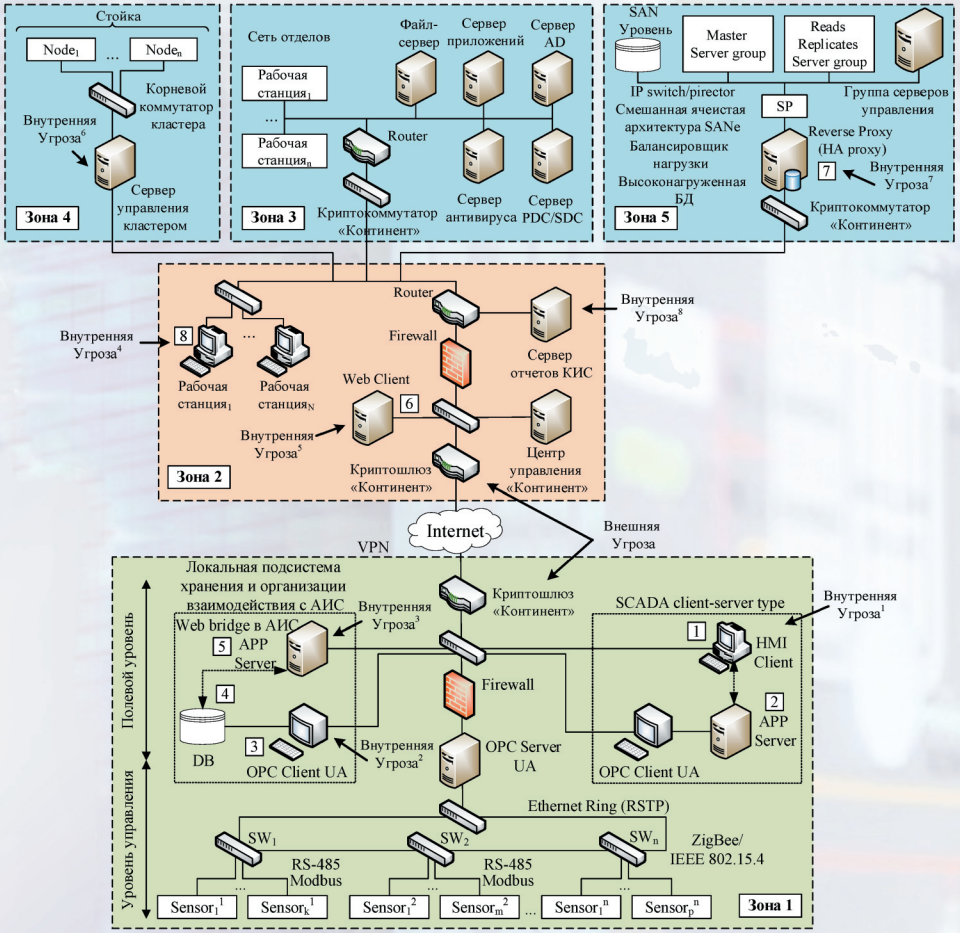

Рис. 2. Структурная схема АИС сбора, хранения и обработки ТМИ

Рисунки к статье В. И. Васильева, А. М. Вульфина, М. Б. Гузаирова, В. М. Картака, Л. Р. Черняховской

«ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ АСУ ТП ПРОМЫШЛЕННЫХ ОБЪЕКТОВ НА ОСНОВЕ ВЛОЖЕННЫХ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ»

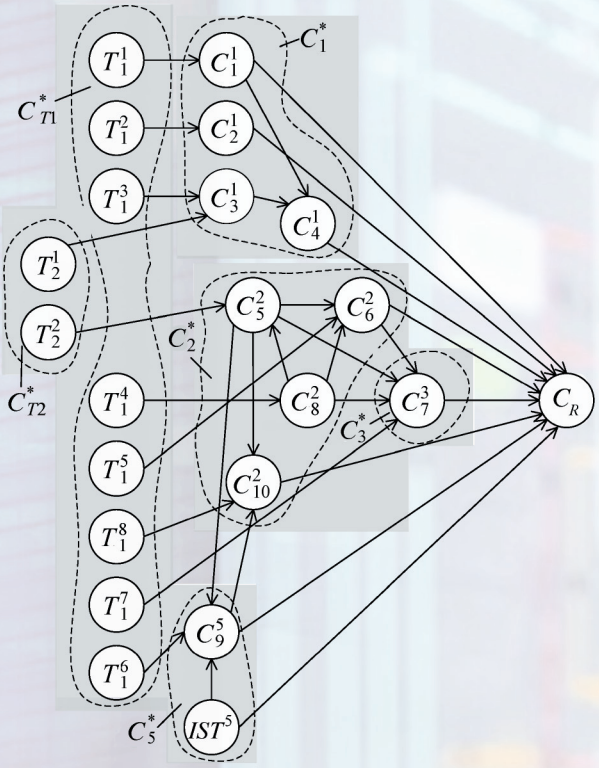

Рис. 4. Первый уровень декомпозиции НСКК для оценки рисков АИС

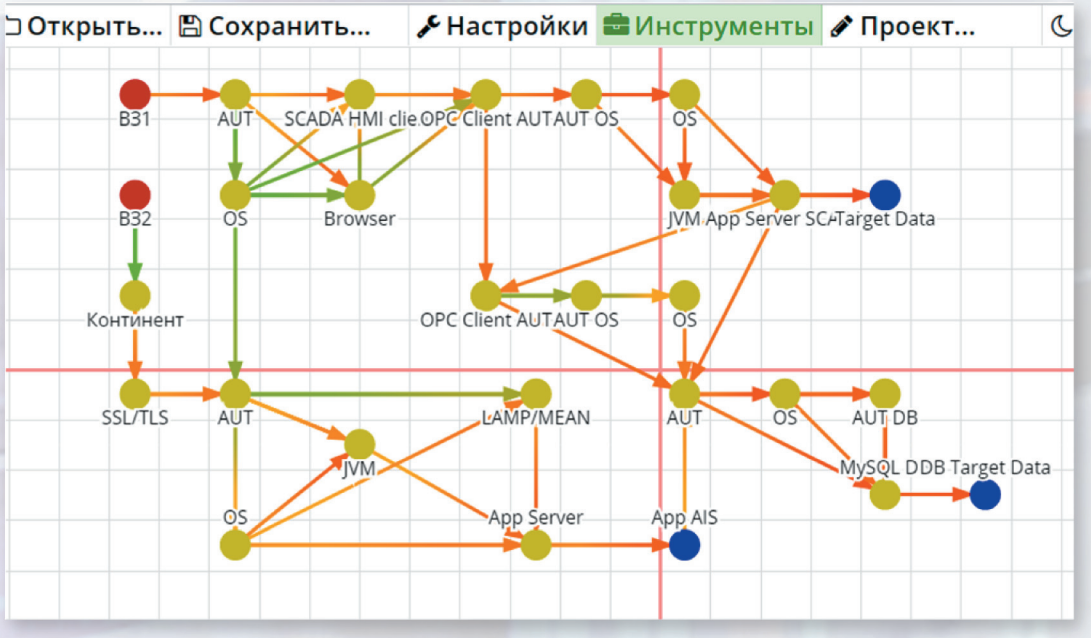

Рис. 6. НСКК для оценки рисков подсистемы сбора и хранения данных на станциях обслуживания (зона 1)