ISSN 2658-5014 (Print)
2023. Т. 5, № 3 (12). С. 77–93
СИИТ
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
ISSN 2686-7044 (Online)
http://siit.ugatu.su

УДК 004.056.5
DOI 10.54708/2658-5014-SIIT-2023-no3-p77

# Оценка рисков информационной безопасности АСУ ТП промышленных объектов методами когнитивного моделирования

**А. Д. Кириллова**

**Аннотация.** В статье представлен обзор результатов исследования автоматизированных систем управления технологическими процессами (АСУ ТП) промышленных объектов. Предметом исследования являются методы, модели и алгоритмы количественной оценки рисков информационной безопасности (ИБ) АСУ ТП промышленных объектов на основе методов когнитивного моделирования. Цель исследования — повышение оперативности и достоверности оценки рисков ИБ АСУ ТП промышленных объектов с использованием технологий когнитивного моделирования и методов машинного обучения. Для достижения цели решаются следующие задачи: 1. Анализ современного состояния проблемы обеспечения ИБ АСУ ТП промышленных объектов с учетом требований существующей нормативно-методической базы. 2. Разработка и исследование нечеткой когнитивной модели количественной оценки рисков ИБ АСУ ТП с учетом воздействия факторов неопределенности и алгоритм ее построения в классе вложенных серых нечетких когнитивных карт. 3. Разработка метода, алгоритма и методики количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе моделирования сценариев атак с использованием технологий когнитивного моделирования и методов машинного обучения. 4. Разработка инструментальных средств автоматизации моделирования сценариев атак на АСУ ТП в составе интеллектуальной системы поддержки принятия решений (ИСППР) на этапе оценки рисков ИБ АСУ ТП промышленных объектов. 5. Разработка методики и практических рекомендаций применения разработанного метода, моделей и алгоритмов оценки рисков ИБ АСУ ТП промышленных объектов для решения прикладных задач. В качестве методов решения использовались методы системного анализа, оценки рисков ИБ, теории графов, когнитивного моделирования и машинного обучения.

**Ключевые слова:** информационная безопасность; оценка рисков; когнитивное моделирование; нечеткие серые когнитивные карты; сценарии атак.

## Введение

Развитие промышленности 4.0 основывается на технологиях промышленного интернета вещей (IIoT) и киберфизических систем, направленных на объединение физического и цифрового производства. Современные промышленные системы автоматизации претерпевают цифровую трансформацию, что существенно обостряет проблему обеспечения информационной безопасности (ИБ) автоматизированных систем управления технологическими процессами (АСУ ТП) промышленных объектов. Внедрение новых технологий, а также унификация и тесная интеграция производства с корпоративной информационной системой и внешней средой влечет за собой возникновение множества новых уязвимостей, угроз и рисков ИБ, ранее не характерных для АСУ ТП.

Об актуальности проблемы обеспечения ИБ АСУ ТП промышленных объектов свидетельствует статистика последних лет [1–3], отражающая стабильный рост числа инцидентов и целенаправленных атак на АСУ ТП с целью промышленного шпионажа, мошенничества и нарушения функционирования предприятия. Так, по материалам исследований «Лаборатории Касперского» [4, 5] во втором полугодии 2022 г. в России зафиксировано самое значительное среди всех стран мира изменение удельного веса (увеличение на 9 %) компьютеров АСУ ТП, подвергшихся компьютерным атакам. С 39,2 % Россия поднялась по этому показателю на тре-

тье место в рейтинге стран. Промышленные системы привлекают нарушителей своими масштабами, значимостью выполняемых бизнес-процессов, их влиянием на окружающий мир и жизнь граждан. В 45 % случаев атаки во втором полугодии 2022 г. привели к нарушению основной деятельности промышленных предприятий, что связано с недоступностью их инфраструктуры в результате атак шифровальщиков. Потеря управления над промышленными объектами может привести к нежелательным последствиям в отдельном субъекте государства или отразиться на экономических показателях страны в целом, а также снизить безопасность жизнедеятельности населения. Соответственно вопросы обеспечения ИБ АСУ ТП промышленных объектов приобретают большое значение. Особое внимание при этом должно уделяться оценке рисков ИБ как необходимой составляющей комплексного подхода к обеспечению ИБ, позволяющей оценить реализуемость сценариев нарушения ИБ и выявить их возможные последствия для построения эффективной системы защиты. За последнее десятилетие активно развивалась нормативно-правовая база обеспечения ИБ АСУ ТП [6–8], но предложенные решения ориентированы, в первую очередь, на качественную оценку рисков ИБ и не позволяют в полной мере ранжировать риски по степени критичности.

Сегодня существенно выросли требования регуляторов, направленные на повышение ИБ АСУ ТП и объектов критической информационной инфраструктуры (КИИ). Необходимо обеспечить частичную или полную автоматизацию процессов обработки больших объемов накапливаемых в современных системах обеспечения ИБ данных о состоянии АСУ ТП промышленных объектов, что позволит в конечном итоге повысить оперативность не только качественной, но и количественной оценки рисков ИБ и будет способствовать повышению защищенности этих объектов в условиях воздействия возможных потенциальных угроз.

Таким образом, тема статьи, является актуальной.

## Степень разработанности темы и обсуждение решаемой задачи

Проблема обеспечения ИБ АСУ ТП отражена в ряде российских и международных нормативно-методических документов, а также в работах ряда российских и зарубежных исследователей. Вопросам обеспечения ИБ АСУ ТП и объектов КИИ посвящены серия стандартов ГОСТ Р 62443, Приказы ФСТЭК России №№ 31, 235, 239, Методика оценки угроз безопасности информации ФСТЭК России от 05.02.2021 г.

Методы оценки рисков ИБ АСУ ТП и объектов КИИ как одного из основных этапов в обеспечении ИБ промышленных систем анализируются в работах И. М. Ажмухамедова, И. В. Аникина, Т. З. Аралбаева, И. И. Баранковой, И. П. Болодуриной, А. С. Катасёва, А. И. Костогрызова, И. И. Лившица, Е. А. Максимовой, Н. Г. Милославской, J. M. Flaus и др. Вместе с тем в настоящее время можно считать отработанными лишь методики качественной оценки рисков ИБ, применяемые для предварительной (качественной) оценки уровня ИБ объекта защиты, а также определенные методики, отражающие общий подход к количественной оценке рисков ИБ и не учитывающие конкретные аспекты, характерные для АСУ ТП промышленных объектов [9–29].

В работах В. И. Васильева, А. М. Вульфина, М. Б. Гузаирова, П. С. Ложникова, И. В. Машкиной, А. А. Шелупанова, J. L. Salmeron, E. I. Papageorgiou и других предложены методы и технологии оценки и анализа рисков ИБ, основанные на использовании новых методов, моделей и технологий интеллектуального анализа данных. Наибольшую сложность в данном случае вызывают недостаточный объем располагаемой статистической информации об угрозах и уязвимостях, ее противоречивость и неполнота, что затрудняет формирование достоверных оценок рисков ИБ и получение итоговых показателей уровня защищенности АСУ ТП.

Вопросы моделирования сценариев компьютерных атак на промышленные системы автоматизации отражены в исследованиях И. В. Котенко, И. Б. Саенко, А. А. Чечулина, S. Noel, A. Yeboah-Ofori, I. Zografopoulos и др. В этих работах предложены инструменты для автоматизации отдельных этапов процесса построения сценариев атак, однако комплексное решение задачи моделирования сценариев атак на АСУ ТП промышленных объектов

с учетом накопленной информации в открытых международных базах знаний до сих пор отсутствует.

Проведенный анализ опубликованных работ в целом показывает, что, несмотря на значительный объем исследований в данной предметной области, проблема адекватной количественной оценки рисков ИБ АСУ ТП и выбора надлежащего состава контрмер нуждается в дальнейшей проработке. По мере увеличения статистических данных и разработки математических моделей риска ИБ, угроз и инцидентов безопасности актуальной становится задача разработки методов и алгоритмов количественной оценки рисков ИБ АСУ ТП, обеспечивающих возможность достоверной оценки уровня защищенности АСУ ТП промышленных объектов и его соответствия требованиям нормативных документов [30].

Объектом исследования являются автоматизированные системы управления технологическими процессами (АСУ ТП) промышленных объектов. Предметом исследования являются методы, модели и алгоритмы количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе методов когнитивного моделирования. Целью исследования является повышение оперативности и достоверности оценки рисков ИБ АСУ ТП промышленных объектов с использованием технологий когнитивного моделирования и методов машинного обучения.

Для достижения поставленной цели решались следующие задачи исследования:

1. Провести анализ современного состояния проблемы обеспечения ИБ АСУ ТП промышленных объектов с учетом требований существующей нормативно-методической базы.

2. Разработать и исследовать нечеткую когнитивную модель количественной оценки рисков ИБ АСУ ТП с учетом воздействия факторов неопределенности и алгоритм ее построения в классе вложенных серых нечетких когнитивных карт.

3. Разработать метод, алгоритм и методику количественной оценки рисков ИБ АСУ ТП промышленных объектов на основе моделирования сценариев атак с использованием технологий когнитивного моделирования и методов машинного обучения.

4. Разработать инструментальные средства автоматизации моделирования сценариев атак на АСУ ТП в составе интеллектуальной системы поддержки принятия решений (ИСППР) на этапе оценки рисков ИБ АСУ ТП промышленных объектов.

5. Разработать методику и практические рекомендации применения разработанного метода, моделей и алгоритмов оценки рисков ИБ АСУ ТП промышленных объектов для решения прикладных задач.

При решении поставленных задач использовались методы системного анализа, оценки рисков ИБ, теории графов, когнитивного моделирования и машинного обучения.

## Анализ современного состояния нормативно-правового и методического обеспечения работ в области ИБ АСУ ТП

Анализ известных методов и алгоритмов оценки рисков ИБ [31–37] показал отсутствие формализованных методик детальной оценки рисков ИБ АСУ ТП промышленных объектов. Существующие нормативные и методические документы в целом направлены на построение статической модели нарушителя, формирование фиксированного перечня угроз, экспертной оценки реализации и уровня значимости угроз. Результаты применения этих методов и алгоритмов затруднительно использовать в практических задачах управления рисками ИБ промышленного предприятия, поскольку они носят, как правило, качественный характер и не позволяют оценить реальные потери от реализации угроз ИБ АСУ ТП и, как следствие, обосновать эффективный выбор контрмер. Кроме того, анализ показал, что их применение осложнено высокой степенью неопределенности и трудоемкости процедуры формализации факторов, влияющих на уровень ИБ АСУ ТП промышленных объектов [38, 39].

## НЕЧЕТКАЯ КОГНИТИВНАЯ МОДЕЛЬ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ РИСКОВ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ФАКТОРОВ НЕОПРЕДЕЛЕННОСТИ И РАЗБРОСА ЭКСПЕРТНЫХ ОЦЕНОК

Характерной особенностью АСУ ТП как объекта защиты является ее многоуровневая иерархическая структура, что определяет специфичность подхода к вопросу обеспечения ИБ автоматизированных промышленных систем [39–41]. Построение моделей АСУ ТП как объекта защиты основано на стандартах серии ГОСТ Р 62443, предусматривающих выделение в рамках иерархической структуры АСУ ряда зон безопасности, связанных между собой трактами. Зональная модель базовой архитектуры АСУ ТП позволяет при этом для распределенных и гетерогенных промышленных систем с большим количеством узлов и уязвимостей производить оценку рисков ИБ не только для отдельных зон, но и для всей системы в целом, позволяя выявить наиболее уязвимые группы информационных ресурсов и обосновать эффективный выбор контрмер.

Разработана функциональная модель процесса оценки рисков ИБ АСУ ТП промышленных объектов (рисунок 1), основанная на Методике оценки угроз безопасности информации ФСТЭК России, в соответствии с которой предложено реализовать данный процесс путем построения иерархии нечетких когнитивных карт применительно к зональной модели АСУ ТП и формализовать таким образом процедуру количественной оценки рисков ИБ АСУ ТП и моделирования сценариев атак как в пределах каждой из зон, так и для всего объекта в целом.

Для реализации процесса оценки рисков ИБ АСУ ТП предложено использовать приведенные в Методике ФСТЭК России и базе знаний MITRE ATT&CK тактики и техники (Tackts, Techs), а также дополнительную информацию из Банка данных угроз безопасности информации (БДУ) ФСТЭК России (Threats) и баз данных шаблонов компьютерных атак (CPE, CVE, CWE, CAPEC) [35]. Использование открытых баз данных угроз и уязвимостей позволяет при этом формально описать сценарии эксплуатации уязвимостей и автоматизировать построение цепочки возможных действий нарушителя на промежуточных узлах АСУ ТП.

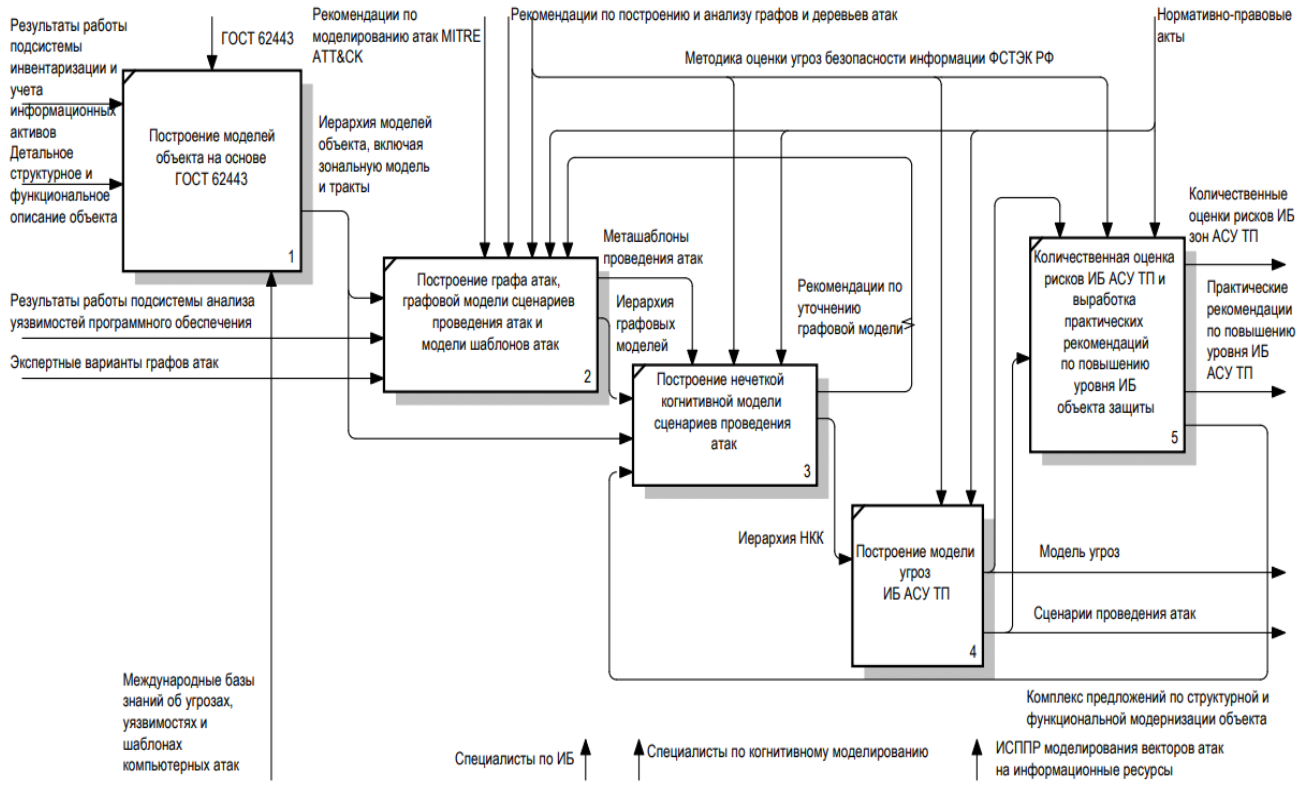



**Рис. 1** Функциональная модель процесса оценки рисков ИБ АСУ ТП промышленных объектов на основе иерархии нечетких когнитивных моделей, формализующих сценарии атак.

Количественная оценка рисков ИБ в пределах каждой выделенной зоны безопасности АСУ ТП основана на построении нечеткой серой когнитивной карты (НСКК) (рисунок 2), которая может быть представлена в виде взвешенного ориентированного графа, заданного с помощью кортежа множеств [42-45]: НСКК $= \langle C, E, W \rangle$, где $C = \{C_i\}$ – множество концептов (вершин графа), $(i = 1,2, \dots, n)$; $E = \{E_{ij}\}$ – множество связей между концептами (дуг графа); $W = \{W_{ij}\}$ – множество весов связей, $(i,j) \in \Omega$. Здесь $\Omega = \{(i_1, j_1), (i_2, j_2), \dots, (i_S, j_S)\}$–множество пар индексов смежных, то есть связанных между собой вершин графа, $S \le n(n-1)$.

Веса связей НСКК и состояния концептов задаются с помощью серых чисел $\otimes W_{ij}$, определяемых как $\otimes W_{ij} \in [\underline{W}_{ij}, \overline{W}_{ij}]$, где $\underline{W}_{ij} < \overline{W}_{ij}, \{\underline{W}_{ij}, \overline{W}_{ij}\} \in [-1,1]$, где $\underline{W}_{ij}$ и $\overline{W}_{ij}$ – соответственно нижняя и верхняя граница серого числа $\otimes W_{ij}$. Таким образом, вес связи между $i$-м и $j$-м концептами $(C_i \to C_j)$ может принимать любое значение в пределах заданного диапазона $[\underline{W}_{ij}, \overline{W}_{ij}] \in [-1,1]$.

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

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

где функции активации концептов $f(\cdot)$ – двухполярные сигмоиды:

$$f(X) = (1 - e^{-x})/(1 + e^{-x}).$$

Значение переменной состояния концепта $C_R$ НСКК определяет итоговую оценку риска ИБ $X_R$ для моделируемых сценариев проведения атак $C_S^1$ и $C_S^2$. Значения весовых коэффициентов $W_{C_C^1, C_S^1}$, $W_{C_C^1, C_S^2}$, $W_{C_C^2, C_S^2}$ характеризуют распределение ограниченных ресурсов на реализацию контрмер $C_C^1$ и $C_C^2$ при моделировании сценариев атак в пределах выделенных зон безопасности АСУ ТП промышленного объекта. Установившиеся значения переменных состояния концептов $C_E^1$ и $C_E^2$ позволяют оценить эффективность интеграции и использования каждой контрмеры.

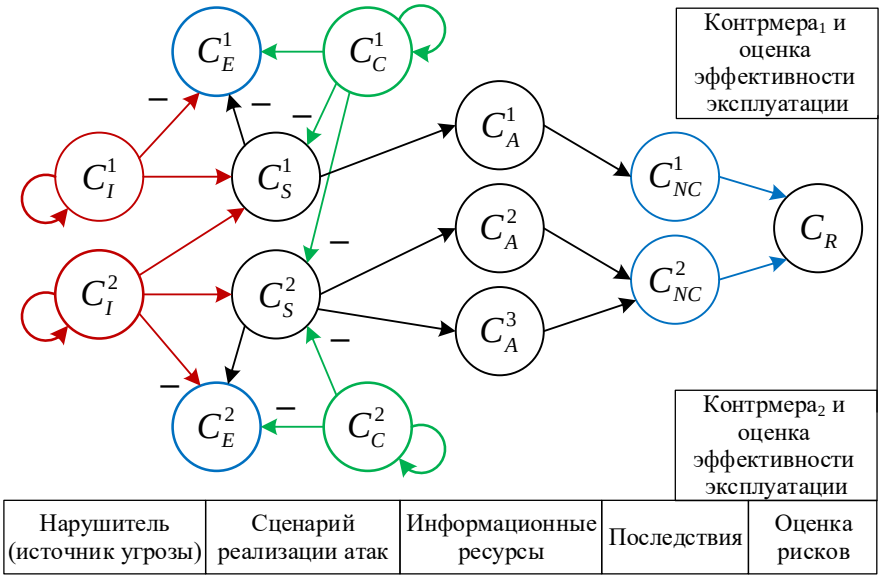



**Рис. 2** НСКК для оценки рисков ИБ АСУ ТП и оценки эффективности распределения ресурсов на реализацию контрмер: $C_I$ – нарушители; $C_E$ – стоимость развертывания и сопровождения контрмер; $C_S$ – выбор способа проведения атаки посредством эксплуатации уязвимостей; $C_A$ – определение информационных ресурсов; $C_{NC}$ – определение негативных последствий для АСУ ТП; $C_C$ – выбор рационального способа защиты с учетом ограничений; $C_R$ – оценка риска ИБ.

Для моделирования возможных действий нарушителя в каждой из выделенных зон безопасности АСУ ТП на различных этапах реализации атаки (наиболее трудоемкий и сложный этап, согласно Методике ФСТЭК) предлагается использовать графовые модели реализации атак, формализуемые с помощью иерархии вложенных НКК. Предложена процедура «сворачивания» исходной детализированной НКК, раскрывающей последовательность действий нарушителя на каждом этапе реализации атаки, до результирующей НКК уровня представления атаки [46, 47].

Алгоритм построения результирующей НКК на основе графовых моделей реализации атаки включает в себя следующие шаги:

1) Построение НКК детализированного уровня графовой модели на основе анализа матрицы переходов между компонентами в пределах одного узла и между узлами выделенной зоны АСУ ТП (рисунок 3, I).

2) Построение НКК для представления различных сценариев атаки (рисунок 3, II).

3) Построение НКК для обобщенного представления варианта проведения отдельной атаки (рисунок 3, III).

4) Построение результирующей НКК (рисунок 4) для моделирования набора возможных сценариев атак на выделенные целевые узлы в пределах отдельных зон и всего объекта в целом с оценкой вероятности реализации и значимости возможных последствий.

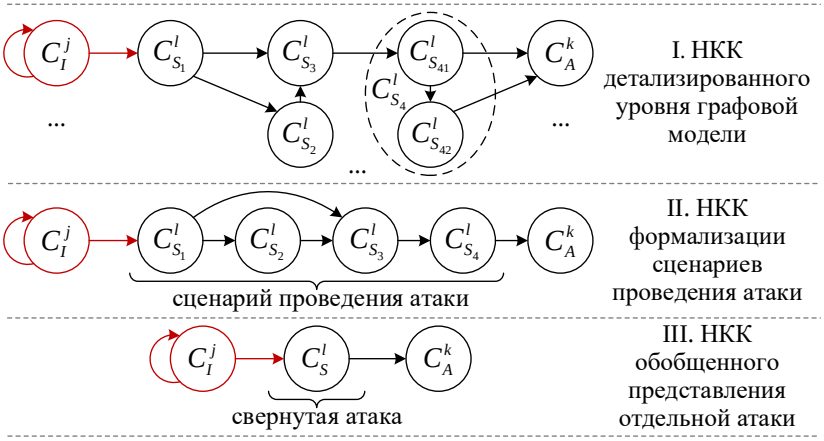



**Рис. 3** Этапы построения результирующей НКК.

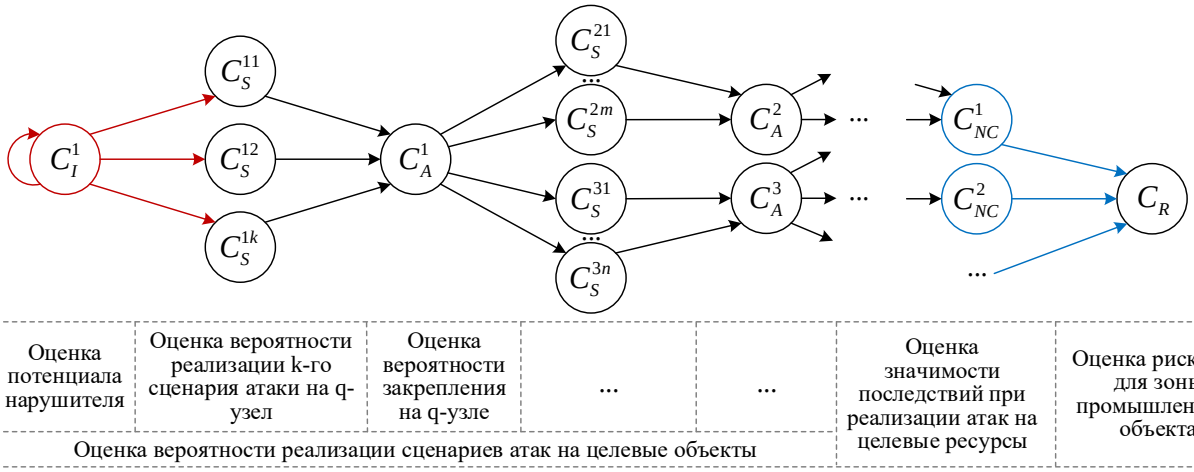



**Рис. 4** НКК для моделирования множества возможных атак на целевые концепты.

Детализированный уровень НКК отражает последовательность возможных действий нарушителя на каждом этапе проведения атаки, что обеспечивает получение развернутой итоговой

оценки рисков ИБ для АСУ ТП. Каждая атака укрупняется до концепта НКК с соответствующими весовыми коэффициентами, позволяющими оценить вероятность ее реализации в каждом из возможных сценариев.

Результирующая НКК позволяет получить оценку рисков ИБ АСУ ТП при реализации нарушителем совокупности атак на целевые ресурсы как в выделенной зоне безопасности объекта, так и для рассматриваемой АСУ ТП в целом.

В [35] рассмотрены особенности использования предложенной методики количественной оценки рисков ИБ с помощью НКК на примере АСУ ТП пункта приема-сдачи подготовленной нефти.

## Метод сценарного моделирования атак

В [35, 43] предложен метод сценарного моделирования атак, реализующий заключительные этапы Методики ФСТЭК России, основанный на построении и анализе комплекса моделей объекта и действий нарушителя, позволяющих формализовать декомпозировать возможные сценарии проведения атак в выделенной зоне безопасности (промышленной сети) АСУ ТП с количественной оценкой соответствующих рисков ИБ.

Иерархия разработанного комплекса моделей представлена на рисунке 5. На основе зональной модели базовой архитектуры АСУ ТП промышленного объекта *1* строится ряд графовых моделей, раскрывающих детали (отдельные аспекты) реализации атаки. Графовые модели сценариев атак *2* формируются на основе графа атак на промышленную сеть *3* (рисунок 6, *а*), перекрестных ссылок и матрицы переходов между выделенными идентификаторами баз данных.

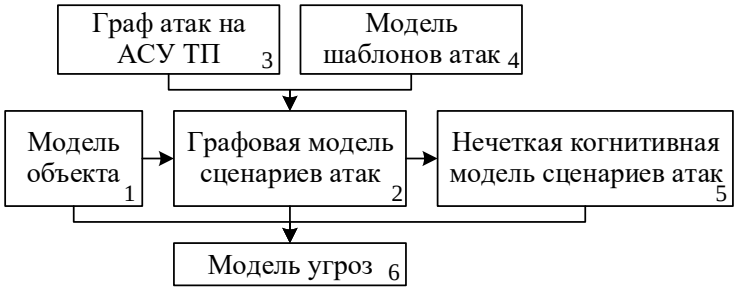
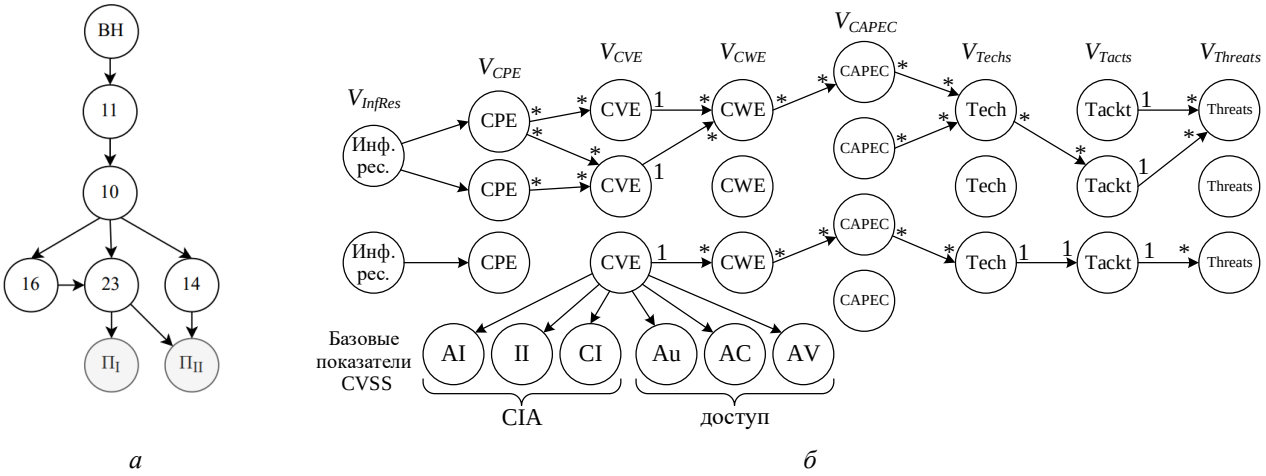



**Рис. 5** Иерархия моделей построения сценариев проведения атак.




*а* *б*

**Рис. 6** Граф атак на промышленную сеть АСУ ТП (*а*) (ВН – нарушитель, $П_1$, $П_2$ – последствия от реализации атак) и графовая модель сценариев проведения атак (*б*), описывающая взаимосвязь CPE-CVE-CWE-CAPEC-ATT&CK.

Графовые модели [48] различной степени детализации строятся исходя из анализа модели объекта, профиля вероятного нарушителя, наиболее вероятных атак и наиболее уязвимых ресурсов системы (рисунок 6, *б*): $V_{\text{InfRes}}$ – множество вершин, соответствующих информационным активам и компонентам АСУ ТП промышленного объекта; $V_{CPE}$ – множество вершин, соответствующих идентификаторам платформ и конфигураций для программно-аппаратного обеспечения системы; $V_{CVE}$ – множество вершин, соответствующих идентификаторам выявленных уязвимостей для каждого элемента системы; $V_{CWE}$ – множество вершин, соответствующих идентификаторам CWE, представляющим недостатки программного и аппаратного обеспечения системы; $V_{CAPEC}$ – множество вершин, соответствующих шаблонам атак CAPEC, описывающим типовые атаки; $V_{Techs}$ – множество вершин, соответствующих техникам реализации атаки, которые описывают инструменты и технологии, используемые в процессе реализации атаки; $V_{Tackts}$ – множество вершин, соответствующих тактикам, то есть действиям нарушителя на различных этапах реализации атаки; $V_{Threats}$ – множество вершин, соответствующих угрозам безопасности информации из БДУ ФСТЭК. Модель шаблонов атак (4) (рисунок 7), построенная на основе открытой базы шаблонов атак CAPEC, используется для детализации графовой модели и анализа возможностей нарушителя, так как графовая модель конструируется в виде цепочки вероятностных переходов между узлами CAPEC (рисунок 8) и представляет собой последовательности действий, совокупность методов и средств, при помощи которых нарушитель достигает поставленной цели воздействия на каждом этапе проведения атаки.

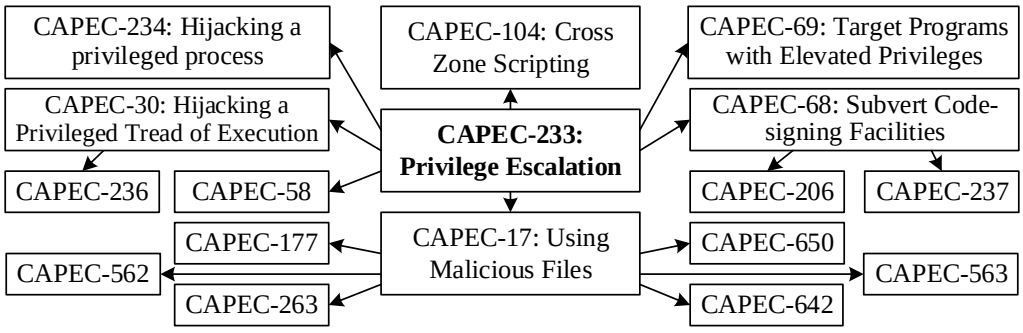



**Рис. 7** Модель шаблонов атак для CAPEC-233.

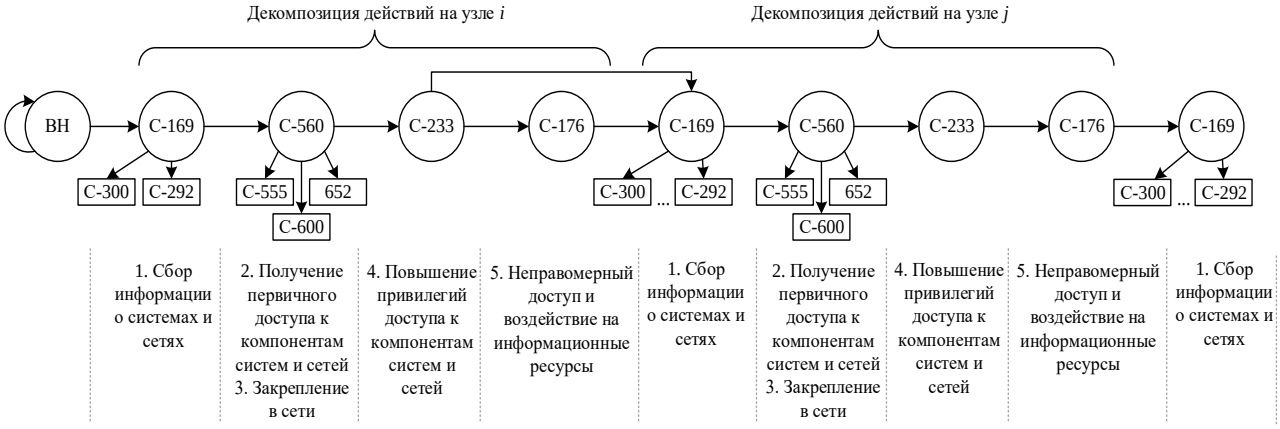



**Рис. 8** Графовая модель проведения атаки на основе шаблонов атак CAPEC.

На рисунке 9 представлена структура подсистемы анализа графовых моделей. Нечеткая когнитивная модель сценариев проведения атаки (5) позволяет анализировать сценарии атак с требуемым уровнем детализации за счет механизмов декомпозиции и композиции действий нарушителя и формировать оценку рисков реализации атаки в целом или на каждом этапе ее исполнения. Модель угроз (6) объединяет всю информацию об объекте, полученную из рас-

смотренных моделей, результаты анализа профиля вероятного нарушителя, а также результаты применения предлагаемого метода сценарного моделирования (перечень актуальных угроз и сценарии их реализации, а также количественную оценку рисков ИБ АСУ ТП).

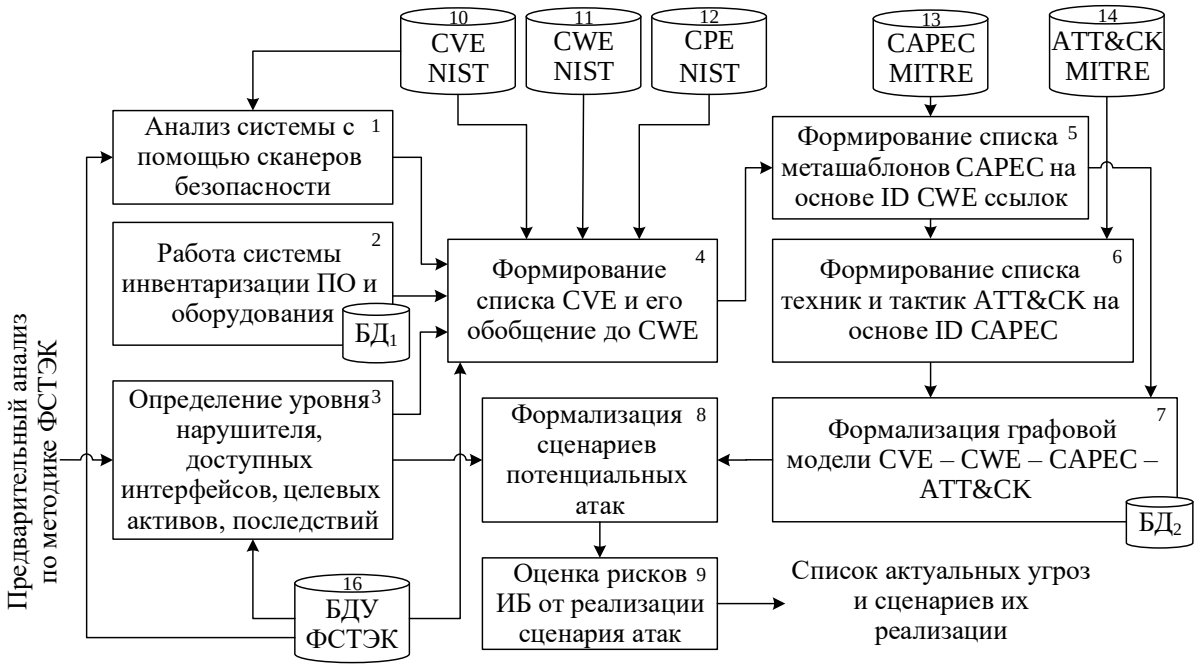



**Рис. 9** Структура подсистемы построения и анализа графовых моделей.

Разработана методика [35] количественной оценки рисков ИБ АСУ ТП на основе нечеткого когнитивного моделирования сценариев атак в выделенных зонах АСУ ТП, позволяющая определить оценки рисков ИБ и оптимальное распределение затрат на реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений.

Приведена формальная постановка задачи многокритериальной оптимизации (2), учитывающей возможность минимизации оценки риска ИБ для выделенной зоны промышленного объекта и оценку эффективности использования контрмер в различных сценариях моделирования при разных вариантах задания целевой функции:

$$X_R \to \min, \quad \sum X_R \to \min, \quad \Phi\left(W_{C_C^i, C_S^j}\right) \to \min, \tag{2}$$

где $\Phi\left(W_{C_C^i, C_S^j}\right)$ – критерий эффективности использования контрмер, $X_R$ – оценка риска ИБ (установившееся значение переменной состояния концепта $C_R$). В качестве оптимизируемых параметров рассматриваются веса НСКК $W_{C_C^i, C_S^j}$, характеризующие распределение выделенных ресурсов на реализацию контрмеры $C_C^i$ с целью снижения вероятности проведения сценария атаки $C_S^j$. Для оптимизации весовых коэффициентов НСКК использован генетический алгоритм (ГА), обеспечивающий нахождение оптимального решения поставленной задачи.

Анализ полученных оценок рисков ИБ в пределах выделенных зон безопасности АСУ ТП и затрат на контрмеры (мероприятия по снижению рисков) [43–51] позволяет определить механизмы управления защищенностью информационных ресурсов объекта и поддерживать необходимый уровень ИБ, а также оценивать требуемые затраты на интеграцию и сопровождение необходимых контрмер. В [36] рассмотрен пример использования предложенной методики сценарного моделирования атак с последующей оценкой рисков ИБ для выделенной зоны АСУ ТП пункта приема-сдачи подготовленной нефти.

### Инструментальные средства автоматизации оценки рисков ИБ

Разработаны инструментальные средства автоматизации оценки рисков ИБ АСУ ТП и моделирования сценариев атак, интегрированные в составе ИСППР. Рассмотрены особенности практического применения полученных результатов, включая анализ угроз и уязвимостей объекта, моделирование сценариев проведения атак на основе открытых баз угроз, уязвимостей и компьютерных атак, построение и визуализацию НКК, с возможностью оптимизации весовых коэффициентов НКК, оценку рисков ИБ в результате возможных действий нарушителя.

Разработанное программное обеспечение (ПО) [46, 47, 49, 53] обеспечивает:

– интеллектуальную поддержку принятия решений при работе с открытыми базами угроз, уязвимостей и шаблонов атак, что позволяет специалистам, выявив конкретные уязвимости объекта, построить наглядную графовую модель реализации атаки (свидетельство о регистрации ПО № 2021614134);

– анализ сценариев проведения атак с требуемым уровнем детализации и оптимизации весовых коэффициентов НКК с помощью методов машинного обучения для решения задачи распределения ресурсов на реализацию контрмер (свидетельство о регистрации ПО № 2021619894).

Представлен фрагмент логической модели данных, описывающей структуру и взаимосвязь основных сущностей предметной области, используемой для создания хранилища данных об угрозах, уязвимостях и сценариях их реализации, а также фрагмент диаграммы классов в нотации UML, раскрывающей имплементацию результатов объектно-ориентированного анализа предметной области моделирования сценариев реализации атак. На рисунке 10 представлен фрагмент архитектуры ИСППР в нотации диаграммы компонентов UML с реализацией патерна MVC.

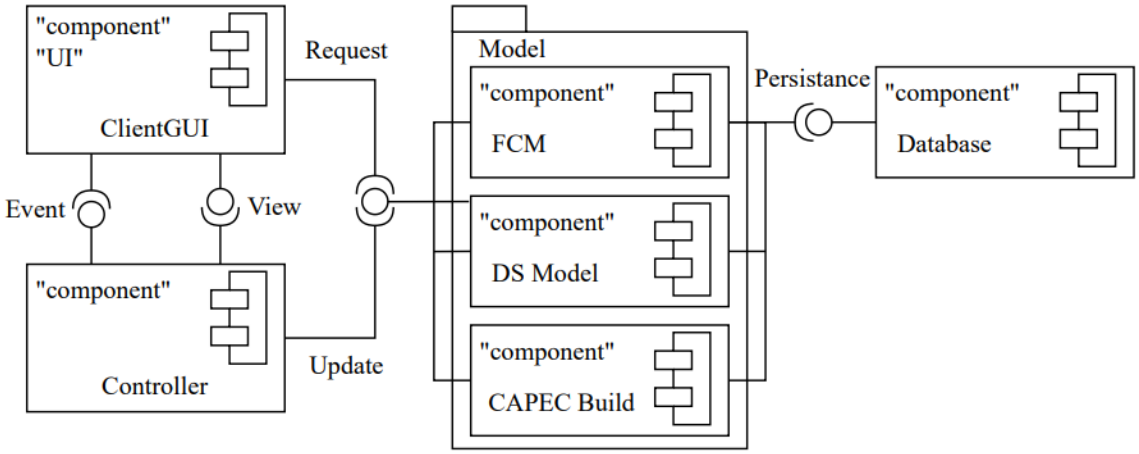



**Рис. 10** Фрагмент архитектуры ИСППР (диаграмма компонентов UML).

Рассмотрен пример применения инструментального средства автоматизации моделирования сценариев атак с последующей оценкой рисков ИБ для АСУ ТП нефтедобывающего предприятия, базовая архитектура которой представлена на рисунке 11. Подсистемы АСУ ТП, согласно терминологии ГОСТ Р 62443, рассматривались в данном случае как отдельные зоны безопасности.

В таблице представлены результаты вычислительных экспериментов по оценке риска ИБ АСУ ТП для различных сценариев проведения атак. С помощью ГА получен набор весовых коэффициентов НСКК, характеризующих оптимальное распределение затрат на реализацию необходимых контрмер по снижению риска ИБ. Величина риска ИБ здесь оценивалась в относительных единицах по отношению к стоимости целевых информационных ресурсов АСУ ТП, эффективность применения контрмер оценивалась по критерию снижения достигнутого уровня риска ИБ.

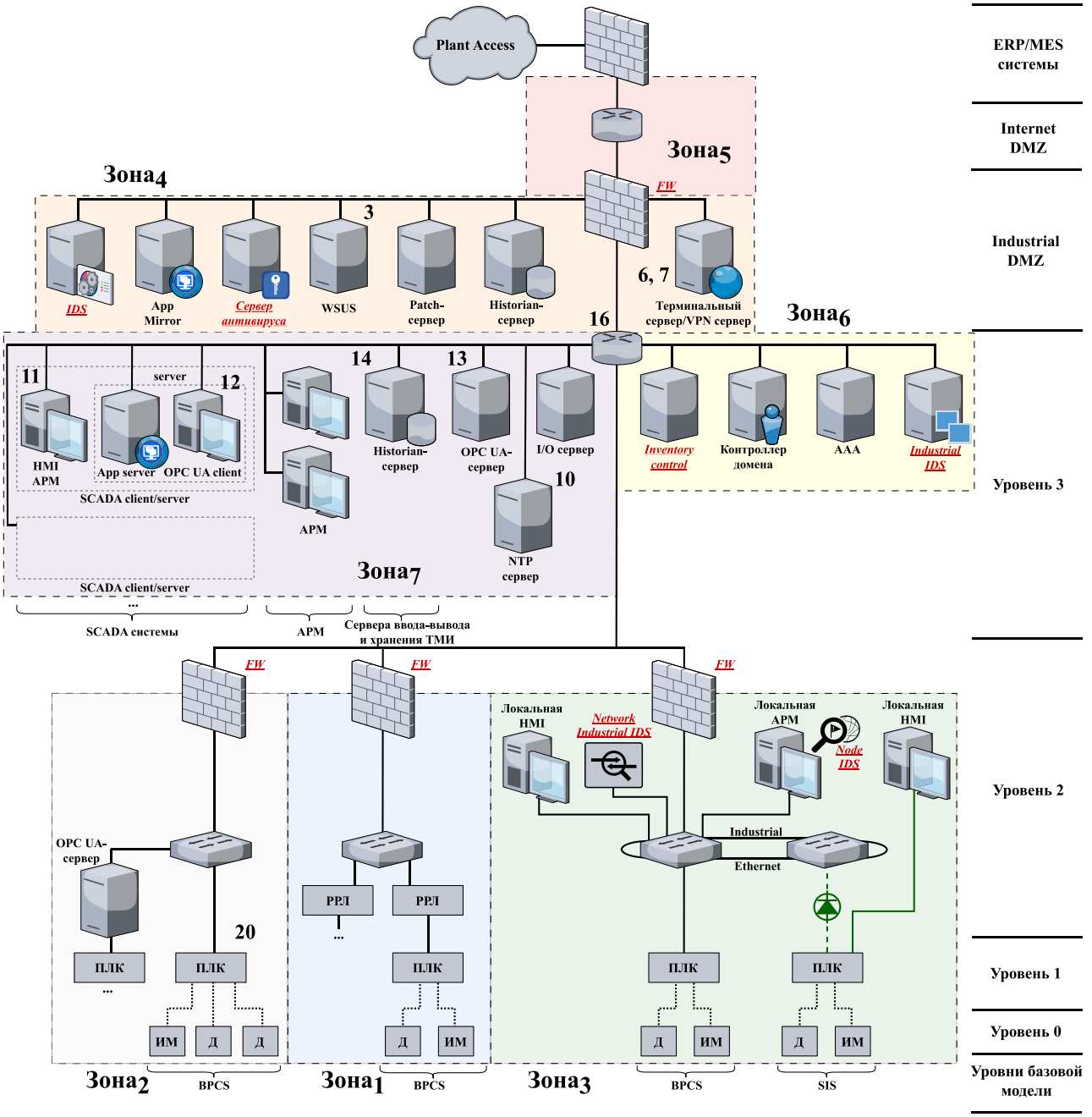



**Рис. 11** Модель базовой архитектуры АСУ ТП нефтедобывающего предприятия.

Таблица

**Результаты оценки рисков ИБ АСУ ТП с оптимизацией весов НСКК**

| Характеристика целевых концептов | Оценка рисков ИБ в диапазоне серых чисел | | |
|---|---|---|---|
| | штатные контрмеры | контрмеры выбраны на основе рекомендаций ИСППР для сценарного уровня моделирования | оптимизация ресурсов контрмер с помощью ГА |
| Оценка риска ИБ для объекта в целом | [0,15; 0,63] | [0,16; 0,52] | [0,09; 0,5] |
| Оценка эффективности применения контрмер | [0,22; 0,72] | [0,3; 0,78] | [0,33; 0,86] |

Сравнение предложенной в работе методики оценки рисков ИБ АСУ ТП с существующими аналогами показало, что применение известных методик осложняется высокой степенью неопределенности в формализации основных факторов, влияющих на защищенность АСУ ТП: появлением новых угроз и уязвимостей, возможностью потери актуальности данных в ходе анализа рисков, что в значительной степени устраняется при использовании предложенной методики.

Дальнейшее направление исследований связано с совершенствованием предложенных алгоритмов, моделей и методик оценки рисков ИБ АСУ ТП и развитием разработанного прототипа ИСППР с целью повышения оперативности и достоверности получения количественных оценок рисков ИБ АСУ ТП для различных промышленных объектов, а также совершенствование методических рекомендаций по выбору эффективного набора контрмер.

## Заключение

1. Проведен анализ современного состояния в области оценки рисков ИБ АСУ ТП. Выявлены достоинства и недостатки существующих методов и алгоритмов оценки рисков применительно к АСУ ТП. Разработана функциональная модель процесса оценки рисков ИБ АСУ ТП, основанная на Методике ФСТЭК России, описывающая процессы формализации зональной модели базовой архитектуры АСУ ТП в виде иерархии нечетких когнитивных карт и формирования количественной оценки рисков ИБ АСУ ТП.

2. Предложены нечеткая когнитивная модель количественной оценки рисков ИБ АСУ ТП промышленных объектов и алгоритм ее построения на основе иерархии вложенных серых нечетких когнитивных карт применительно к зональной модели базовой архитектуры АСУ ТП, которая, в отличие от существующих методов и подходов оценки рисков ИБ, учитывает многоуровневую организацию промышленных объектов и позволяет формализовать сценарии атак с требуемым уровнем детализации в пределах выделенных зон, что позволяет повысить достоверность и обоснованность количественной оценки рисков ИБ и, как следствие, обеспечить обоснованный выбор эффективных контрмер.

3. Разработан метод количественной оценки рисков ИБ АСУ ТП на основе моделирования сценариев атак с использованием технологий когнитивного моделирования и методов машинного обучения, позволяющий получить формализованное описание объекта атаки, перечня актуальных угроз и уязвимостей в виде иерархии графовых моделей, что существенно повышает обоснованность и полноту сценарного моделирования за счет представления последовательности тактик и техник, позволяющих нарушителю реализовать атаку на АСУ ТП. Решается задача оптимизации параметров когнитивных моделей, отражающих распределение затрат на реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений. Оптимизация распределения ресурсов, выделенных на контрмеры, позволяет повысить эффективность эксплуатации контрмер и снизить количественную оценку риска ИБ для объекта защиты в целом.

4. Разработаны алгоритмы и методика количественной оценки рисков ИБ АСУ ТП на основе построения сценариев атак, отличающиеся применением нечеткого когнитивного моделирования и методов машинного обучения для оценки уровня защищенности выделенных зон АСУ ТП. Анализ сценариев атак с требуемым уровнем детализации действий нарушителя позволяет формировать оценку рисков реализации атаки в целом или на каждом этапе ее исполнения. Предложена методика количественной оценки рисков ИБ АСУ ТП на основе нечеткого когнитивного моделирования сценариев атак в выделенных зонах АСУ ТП промышленного объекта, позволяющая определить оценки рисков ИБ и оптимальное распределение затрат на реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений.

5. Разработаны архитектура исследовательского прототипа ИССПР и программная реализация инструментальных средств автоматизации оценки рисков ИБ и моделирования сценариев атак, позволяющая извлечь информацию о слабых местах инфраструктуры АСУ ТП,

наиболее опасных уязвимостях и потенциальных слабостях компонент системы, выявить наиболее успешные потенциальные сценарии атак, оценить их последствия для промышленного предприятия.

6. Разработаны методика и практические рекомендации применения разработанного метода, моделей, алгоритмов и инструментальных средств оценки рисков ИБ АСУ ТП промышленных объектов для решения прикладных задач. Проведенные вычислительные эксперименты показали, что на этапах проектирования и внедрения контрмер временные затраты на моделирование сценариев реализации атак сократились более чем в 2,5 раза; на 15 % повысилась эффективность эксплуатации контрмер за счет оптимизации распределения ресурсов их применения; на 10 % снизилась количественная оценка уровня риска ИБ для объекта защиты в целом; предложенные решения позволяют сформировать расширенный список контрмер на основе баз знаний БДУ ФСТЭК России, ATT&CK, NVD для каждой из выделенных зон безопасности.

**СПИСОК ЛИТЕРАТУРЫ / REFERENCES**

1. Claroty Biannual ICS Risk & Vulnerability Report: 1H 2021 [Online]. Available: https://claroty.com/wp-content/uploads/2021/08/Claroty_Biannual_ICS_Risk_Vulnerability_Report_1H_2021.pdf [Accessed Aug. 15, 2023].

2. Spring J., Hatleback E., Householder A., Manion A. and Shick D. Time to Change the CVSS? // IEEE Security & Privacy. Vol. 19. No. 2. Pp. 74–78, 2021.

3. Исследования. Аналитики Positive Technologies [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ (дата обращения: 15.08.2023). [[ Research. Analysts at Positive Technologies [Online], (in Russian). URL: https://www.ptsecurity.com/ru-ru/research/analytics/ (2023, Aug. 15) ]]

4. Ландшафт угроз для систем промышленной автоматизации в России. Ответы, которые мы знаем [Электронный ресурс]. URL: https://ics-cert.kaspersky.ru/publications/reports/2022/09/20/threat-landscape-for-industrial-automation-systems-in-russia/ (дата обращения: 15.08.2023). [[ Threat Landscape for Industrial Automation Systems in Russia. The Answers We Know [Online], (in Russian). URL: https://ics-cert.kaspersky.ru/publications/reports/2022/09/20/threat-landscape-for-industrial-automation-systems-in-russia/ (2023, Aug. 15) ]]

5. Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2022 [Электронный ресурс]. URL: https://ics-cert.kaspersky.ru/publications/reports/2023/03/06/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2022/ (дата обращения: 15.08.2023). [[ Threat Landscape for Industrial Automation Systems. Statistics for H2 2022 [Online], (in Russian). URL: https://ics-cert.kaspersky.ru/publications/reports/2023/03/06/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2022/ (2023, Aug. 15) ]]

6. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей среды (утверждены приказом ФСТЭК России от 14.03.2014 № 31). М., 2014. [Электронный ресурс].URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (дата обращения: 15.08.2023). [[ Requirements for Ensuring the Protection of Information in Automated Control Systems for Production and Technological Processes at Critically Important Facilities, Potentially Hazardous Facilities, as well as Facilities that Pose an Increased Danger to the Life and Health of People and the Environment (approved by order of the FSTEC of Russia dated March 14, 2014, No. 31). Moscow, 2014. [Online], (in Russian). URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (2023, Aug. 15) ]]

7. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утверждены приказом ФСТЭК России от 25.12.2017 г. № 239). М., 2017. [Электронный ресурс]. URL: https://fstec.ru/component/attachments/download/1880 (дата обращения: 15.08.2023). [[ Requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation (approved by order of the FSTEC of Russia dated December 25, 2017, No. 239). Moscow: 2017. [Online], (in Russian). URL: https://fstec.ru/component/attachments/download/1880 (2023, Aug. 15) ]]

8. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (дата обращения: 15.08.2023). [[ Federal Law No. 187-FZ “On the security of critical information infrastructure of the Russian Federation” dated July 26, 2017 [Online], (in Russian). URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (2023, Aug. 15) ]]

9. Жумажанова С. С., Сулавко А. Е., Ложников П. С. Распознавание психофизиологического состояния субъектов-операторов на основе анализа термографических изображений лица с применением сверточных нейронных сетей // Системная инженерия и информационные технологии. 2023. Т. 5. № 2(11). С. 41–55. [[ S. S. Zhumazhanova, A. E. Sulavko and P. S. Lozhnikov. Recognition of the psychophysiological state of subject-operators based on the analysis of thermographic images of the face using convolutional neural networks (in Russian) // Systems Engineering and Information Technologies, vol. 5, no. 2(11), pp. 41-55, 2023. ]]

10. Братченко А. И., Бутусов И. В., Кобелян А. М., Романов А. А. Применение методов теории нечетких множеств к оценке рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления // Вопросы кибербезопасности. 2019. № 1 (29). С. 18–24. [[ A. I. Bratchenko, I. V. Butusov, A. M. Kobalyan and A. A. Romanov. Application of

methods of theory of fuzzy sets to assess the risk of violations of critical properties protected resources automated control system (in Russian) // Cybersecurity Issues, no. 1(29), pp. 18-24, 2019. ]]

11. Булдакова Т. И., Миков Д. А. Методика анализа информационных рисков с применением нейро-нечеткой сети // НТИ. Сер. 2. Информационные процессы и системы. 2015. № 4. С. 13–17. [[ T. I. Buldakova and D. A. Mikov. Methodology for analyzing information risks using a neuro-fuzzy network (in Russian) // NTI. Ser. 2. Information processes and systems, no. 4, pp. 13-17, 2015. ]]

12. Васильев В. И., Гузаиров М. Б., Вульфин А. М. Оценка рисков информационной безопасности с использованием нечетких продукционных когнитивных карт // Информационные технологии. 2018. Т. 24. № 4. С. 266–273. [[ V. I. Vasilyev, M. B. Guzairov and A. M. Vulfin. Evaluation of information security risks with use of rule-based fuzzy cognitive maps (in Russian), // Information Technology, vol. 24, no. 4, pp. 266-273, 2018. ]]

13. Васильев В. И., Вульфин А. М., Гузаиров М. Б., Картак В. М., Черняховская Л. Р. Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт // Информационные технологии. 2020. Т. 26. № 4. С. 213–221. [[ V. I. Vasilyev, A. M. Vulfin, M. B. Guzairov, V. M. Kartak and L. R. Chernyakhovskaya. Assessment of cybersecurity risks of automated process control systems of industrial facilities based on nested fuzzy cognitive maps (in Russian) // Information Technology, vol. 26, no. 4, pp. 213-221, 2020. ]]

14. Гарбук С. В., Правиков Д. И., Полянский А. В., Самарин И. В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты // Вопросы кибербезопасности. 2019. № 3 (31). С. 63–71. [[ S. V. Garbuk, D. I. Pravikov, A. V. Polyansky, and I. V. Samarin. Ensurin APCS information security using the predictive protection method (in Russian) // Cybersecurity Issues, no. 3(31), pp. 63-71, 2019. ]]

15. Гаськова Д. А., Массель А. Г. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. № 2 (30). С. 42–49. [[D. A. Gaskova and A. G. Massel. The technology of cyber threat analysis and risk assessment of cybersecurity violation of critical infrastructure (in Russian) // Cybersecurity Issues, no. 2(30), pp. 42-49, 2019. ]]

16. Ильченко Л. М., Брагина Е. К., Егоров И. Е., Зайцев С. Ю. Расчет рисков информационной безопасности телекоммуникационного предприятия // Открытое образование. 2018. Т. 22. № 2. С. 61–70. [[ L. M. Ilchenko, E. K. Bragina, I. E. Egorov, and S. I. Zaysev. Calculation of risks of information security of telecommunication enterprise (in Russian) // Open Education, vol. 22, no. 2, pp. 61-70, 2018. ]]

17. Кирилина Т. Ю., Горбанева Е. Н., Познякевич А. В. Нормативно-правовое регулирование информационной безопасности автоматизированных систем управления технологическими процессами // Информационно-технологический вестник. 2018. № 2 (16). С. 78–85. [[ T. Yu. Kirilina, E. N. Gorbaneva and A. V. Poznyakevich. Legal and regulatory framework of information security of automated process control systems (in Russian) // Information Technology Bulletin, no. 2(16), pp. 78-85, 2018. ]]

18. Каменских А. Н., Бортник Д. А. Анализ рекомендаций по защите автоматизированных систем управления с целью выявления типичных уязвимостей // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. 2016. №. 17. С. 48–60. [[ A. N. Kamenskih and D. A. Bortnik. Analysis of guide to ICS security to identify the typical vulnerabilities (in Russian) // PNRPU Bulletin. Electrotechnics, Informational Technologies, Control Systems, no. 17, pp. 48-60, 2016. ]]

19. Кирсанов С. В. Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли // Доклады ТУСУР. 2013. №. 2 (28). С. 112–115. [[ S. V. Kirsanov. The method for assessment of information security threats for APCS of the gas industry (in Russian) // Proceedings of TUSUR University, no. 2(28), pp. 112-115, 2013. ]]

20. Колосок И. Н., Гурина Л. А. Оценка рисков кибербезопасности информационно-коммуникационной инфраструктуры интеллектуальной энергетической системы // Информационные и математические технологии в науке и управлении. 2019. №. 2 (14). С. 40–51. [[ I. N. Kolosok, L. A. Gurina. Cybersecurity risk assessment of information and communication infrastructure of intelligent energy system (in Russian) // Information and Mathematical Technologies in Science and Management, no. 2(14), pp. 40-51, 2019. ]]

21. Костогрызов А. И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии // Вопросы кибербезопасности. 2022. № 6. (52). С. 71–82. [[ A. I. Kostogryzov. On models and methods of probabilistic analysis of information security in standardized systems engineering processes (in Russian) // Cybersecurity Issues, no. 6(52), pp. 71-82, 2022. ]]

22. Лившиц И. И., Бакшеев А. С. Исследование методик контроля уровня защищенности информации на объектах критической информационной инфраструктуры // Вопросы кибербезопасности. 2022. №. 6. (52). С. 40–52. [[ I. I. Livshitz and A. S. Baksheev. Research of methods for monitoring the level of information security at critical information infrastructure facilities (in Russian) // Cybersecurity Issues, no. 6(52), pp. 40-52, 2022. ]]

23. Массель А. Г., Гаськова Д. А. Онтологический инжиниринг для разработки интеллектуальной системы анализа угроз и оценки рисков кибербезопасности энергетических объектов // Онтология проектирования. 2019. №. 2 (32). С. 225–238. [[ A. G. Massel and D. A. Gaskova. Ontological engineering for the development of an intelligent system for threat analysis and risk assessment of cybersecurity of energy facilities (in Russian) // Ontology of Designing, no. 2(32), pp. 225-238, 2019. ]]

24. Asghar M. R., Hu Q. and Zeadally S. Cybersecurity in industrial control systems: Issues, technologies, and challenges // Computer Networks. 2019. Vol. 165. Pp. 106946.

25. Barankova I. I., Mikhailova U. V. and Kalugina O. B. Analysis of the problems of industrial enterprises information security audit//Proceedings of the International Russian Automation Conference Advances in Automation. Springer International Publishing, 2020. Pp. 976–985.

26. Bhamare D., Zolanvari M., Erbad A., Jain R., Khan K. and Meskin N. Cybersecurity for industrial control systems: A survey// Computers & Security. 2020. Vol. 89. Pp. 101677.

27. Efimov B. I. and Lozhnikov P. S. Analysis of the impact of threats to change and block responses of experts in online survey systems // Journal of Physics: Conference Series. IOP Publishing. 2020. Vol. 1546. No. 1. Pp. 012079.

28. Hu J., Guo S., Kuang X., Meng F., Hu D. and Shi Z. I-hmm-based multidimensional network security risk assessment// IEEE Access. 2020. Vol. 8. Pp. 1431–1442.

29. Maksimova E. A. and Baranov V. V. Predicting Destructive Malicious Impacts on the Subject of Critical Information Infrastructure //Futuristic Trends in Network and Communication Technologies, 2021. Pp. 88–99.

30. Махмутов А. Р., Вульфин А. М., Миронов К. В. Исследование возможностей автономной работы конечных устройств интернета вещей // Системная инженерия и информационные технологии. 2023. Т. 5. № 1(10). С. 41–47. [[ A. R. Makhmutov, A. M. Vulfin, K. V. Mironov. Research of the autonomous operation time of IoT end devices (in Russian) // Systems Engineering and Information Technologies, vol. 5, no. 1(10), pp. 41-47, 2023. ]]

31. Аникин И. В. Методы и алгоритмы количественной оценки и управления рисками безопасности в корпоративных информационных сетях на основе нечеткой логики // Системная инженерия и информационные технологии. 2023. Т. 5. № 3(12). С. 93–113. [[ I. V. Anikin. Methods and algorithms for quantitative assessment and management of security risks in corporate information networks based on fuzzy logic (in Russian) // Systems Engineering and Information Technologies, vol. 5, no. 3(12), pp. 93-113, 2023. ]]

32. 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. DOI: 10.14529/secur180410. [[ V. I. Vasilyev, A. D. Kirillova and S. N. Kukharev. Cybersecurity of APCS: modern trends and approaches (current state, perspectives) (in Russian) // Vestnik UrFO. Security in the Information Sphere, vol. 4(30), pp. 66-74. DOI: 10.14529/secur180410. ]]

33. Васильев В. И., Вульфин А. М., Кириллова А. Д., Черняховская Л. Р. Об интерпретируемости нечетких когнитивных моделей на этапе оценки рисков инновационных проектов // Вестник УрФО. Безопасность в информационной сфере. 2019. № 4(34). С. 45–57. [[ V. I. Vasilyev, A. M. Vulfin, A. D. Kirillova and L. R. Chernyakhovskaya. On the interpretability of fuzzy cognitive models at the stage of risks assessment for innovative projects (in Russian) // Vestnik UrFO. Security in the Information Sphere, vol. 4(34), pp. 45-57, 2019. ]]

34. Васильев В. И., Вульфин А. М., Кириллова А. Д., Кучкарова Н. В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. 2021. № 3. С. 110–134. [[ V. I. Vasilyev, A. M. Vulfin, A. D. Kirillova and N. V. Kuchkarova. Methodology for assessing current threats and vulnerabilities based on cognitive modeling technologies and Text Mining (in Russian) // Systems of Control, Communication and Security, no. 3, pp. 110-134, 2021. ]]

35. Васильев В. И., Кириллова А. Д., Вульфин А. М. Когнитивное моделирование вектора кибератак на основе меташаблонов CAPEC // Вопросы кибербезопасности. 2021. № 2(42). С. 2–16. [[ V. I. Vasilyev, A. D. Kirillova and A. M. Vulfin. Cognitive modeling of the cyber attack vector based on CAPEC methods (in Russian) // Cybersecurity Issues, vol. 2(42), pp. 2-16, 2021. ]]

36. Васильев В. И., Вульфин А. М., Кириллова А. Д. Анализ и управление рисками информационной безопасности АСУ ТП на основе когнитивного моделирования // Моделирование, оптимизация и информационные технологии. 2022. Т. 10. № 2(37). С. 1–18. DOI 10.26102/2310-6018/2022.37.2.022. URL: https://moitvivt.ru/ru/journal/pdf?id=1184 (дата обращения: 15.08.2023). [[ V. I. Vasilyev, A. M. Vulfin and A. D. Kirillova. Analysis and management of ICS cybersecurity risks based on cognitive modeling [Online], (in Russian) // Modeling, Optimization and Information Technology, no. 8(2), pp. 1-16, 2020. DOI: 10.26102/2310-6018/2022.37.2.022. URL: https://moitvivt.ru/ru/journal/pdf?id=1184 (2023, Aug. 15) ]]

37. Васильев В. И., Вульфин А. М., Гузаиров М. Б., Кириллова А. Д. Комплексная оценка выполнения требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами // Инфокоммуникационные технологии. 2017. Т. 15. № 4. С. 319–325. DOI: 10.18469/ikt.2017.15.4.02. [[ V. I. Vasilyev, A. M. Vulfin, M. B. Guzairov and A. D. Kirillova. Integrated assessment of information security requirements implementation in automated control systems intended for production and technological processes (in Russian) // Infokommunikacionnye Tehnologii, vol. 15, no. 4, pp. 319-325, 2017. ]]

38. Кириллова А. Д. Экспертная система аудита информационной безопасности АСУ ТП // Материалы V Всероссийской конференции «Информационные технологии интеллектуальной поддержки принятия решений». 2017. Т. 2. С. 172–175. [[ A. D. Kirillova Expert system for auditing information security of automated process control systems (in Russian) // In: Proceedings of the 5th All-Russian Conference on Information Technologies for Intelligent Decision Making Support, 2017, vol. 2, pp. 172-175.]]

39. Kirillova A. D., Vasilyev V. I., Nikonov A. V. and Berkholts V. V. Decision support system in the task of ensuring information security of automated process control systems // Proceedings of the Data Science Session at the 5th International Conference on Information Technology and Nanotechnology. CEUR Workshop, 2019. Pp. 477–486. DOI: 10.18287/1613-0073-2019-2416-477-486.

40. Васильев В. И., Гвоздев В. Е., Гузаиров М. Б., Кириллова А. Д. Система поддержки принятия решений по обеспечению информационной безопасности автоматизированной системы управления технологическими процессами // Информация и безопасность. 2017. Т. 20. № 4. С. 618–623. [[ V. I. Vasilyev, V. E. Gvozdev, M. B. Guzairov and A. D. Kirillova Decision support system for ensuring information security of an automated process control system (in Russian) // Information and Security, vol. 20, no. 4, pp. 618-623, 2017. ]]

41. Гузаиров М. Б., Фрид А. И., Вульфин А. М., Берхольц В. В., Кириллова А. Д. Анализ защищенности системы сбора, хранения и обработки телеметрической информации о состоянии бортовых систем летательного аппарата // Вестник УГАТУ. 2019. Т. 23. № 4(86). С. 132–146. [[ M. B. Guzairov, A. I. Frid, A. M. Vulfin, V. V. Berkholts and A. D. Kirillova Analysis of the protection of the collection, storage and processing of telemetric information on the condition of airplane systems (in Russian) // Vestnik UGATU, vol. 23, no. 4(86), pp. 132-146, 2019. ]]

42. 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. Т. 24. № 10. С. 657–664. [[ V. I. Vasilyev, A. M. Vulfin, M. B. Guzairov and A. D. Kirillova Interval estimation of information risks with use of fuzzy grey cognitive maps (in Russian) // Information Technologies, vol. 24, no. 10, pp. 657-664, 2018. ]]

43. Vasilyev V. I., Kirillova A. D., Vulfin A. M. and Nikonov A. V. Cybersecurity risk assessment based on cognitive attack vector modeling with CVSS Score // 2021 International Conference on Information Technology and Nanotechnology (ITNT). IEEE, 2021. Pp. 1–6. DOI: 10.1109/ITNT52450.2021.9649191.

44. Гузаиров М. Б., Вульфин А. М., Картак В. М., Кириллова А. Д., Миронов К. В. Сравнительный анализ алгоритмов когнитивного моделирования при оценке рисков информационной безопасности // Труды ИСА РАН. 2019. Т. 69. № 4. С. 62–69. [[ M. B. Guzairov, A. M. Vulfin, V. M. Kartak, A. D. Kirillova and K. V. Mironov. Comparative analysis of algorithms for cognitive modeling in assessing information security risks (in Russian) // Proceedings of the ISA RAS, vol. 69, no. 4, pp. 62-69, 2019. ]]

45. Васильев В. И., Вульфин А. М., Берхольц В. В., Кириллова А. Д., Бельский С. М. Анализ рисков обеспечения целостности телеметрической информации с использованием технологии когнитивного моделирования // Вестник УГАТУ. 2019. Т. 23. № 4(86). С. 122–131. [[ V. I. Vasilyev, A. M. Vulfin, V. V. Berkholts, A. D. Kirillova, and S. M. Belskii. Risk analysis for ensuring the integrity of telemetric information using cognitive modeling technology (in Russian) // Vestnik UGATU, vol. 23б no. 4(86), pp. 122-131, 2019. ]]

46. Вульфин А. М., Ягафаров Р. Р., Кириллова А. Д., Васильев В. И. Программа моделирования нечетких когнитивных карт: свидетельство о государственной регистрации программы для ЭВМ 2021615069 Российская Федерация. № 2021614134/заявл. 26.03.2021; опубл. 02.04.2021. [[ A. M. Vulfin, R. R. Yagafarov, A. D. Kirillova and V. I. Vasilyev. Program for modeling fuzzy cognitive maps: Certificate of state registration of the computer program 2021615069 Russian Federation. No. 2021614134; application 26.03.2021; publ. 02.04.2021. ]]

47. Кириллова А. Д., Вульфин А. М., Ягафаров Р. Р., Зиязетдинова Л. Ю. Программа анализа и моделирования кибератак на основе меташаблонов в нечетком когнитивном базисе: свидетельство о государственной регистрации программы для ЭВМ 2021619894 Российская Федерация. № 2021618903; заявл. 07.06.2021; опубл. 18.06.2021. [[ A. D. Kirillova, A. M. Vulfin, R. R. Yagafarov, and L. Yu. Ziyazetdinova. A program for analyzing and modeling cyber attacks based on meta-patterns in a fuzzy cognitive basis: Certificate of state registration of the computer program 2021619894 Russian Federation. No. 2021618903; application 07.06.2021; publ. 18.06.2021. ]]

48. Гаянова М. М., Вульфин А. М. Структурно-семантический анализ научных публикаций выделенной предметной области // Системная инженерия и информационные технологии. 2022. Т. 4. № 1(8). С. 37–43. [[ M. M. Gayanova and A. M. Vulfin. Structural and semantic analysis of scientific publications in a selected subject area (in Russian) // Systems Engineering and In-formation Technologies, vol. 4, no. 1, pp. 37-43, 2022. ]]

49. Вульфин А. М., Никонов А. В., Габбасова Д. Н. и др. Программа анализа уязвимостей программного обеспечения на основе технологий интеллектуального анализа и обработки естественного языка: свидетельство о государственной регистрации программы для ЭВМ 2021615080 Российская Федерация. № 2021614120; заявл. 26.03.2021; опубл. 02.04.2021. [[ A. M. Vulfin, A. V. Nikonov, D. N. Gabbasova, et al. Software vulnerability analysis program based on mining and natural language processing technologies: Certificate of state registration of a computer program 2021615080 Russian Federation. No. 2021614120; application 26.03.2021; publ. 02.04.2021 ]]

50. Hajrullin E. R., Vulfin A. M., Mironov K. V., Frid A. I., Guzairov M. B. and Kirillova A. D. Secure data exchange in the industrial inter-net of things network of the fuel and energy complex// Proceedings ICOECS 2020 International Conference on Electro-technical Complexes and Systems. IEEE, 2020. Pp. 353–358.

51. Vulfin A. M., Vasilyev V. I., Kuharev S. N., Homutov E. V. and Kirillova A. D. Algorithms for detecting network attacks in an enter-prise industrial network based on data mining algorithms // Journal of Physics: Conference Series. IOP Publishing. 2021. Vol. 2001. Pp. 012004.

52. Васильев В. И., Вульфин А. М., Картак В. М., Кириллова А. Д., Миронов К. В. Система обнаружения атак в беспроводных сенсорных сетях промышленного интернета вещей // Труды ИСА РАН. 2019. Т. 69. № 4. С. 70–78. [[ V. I. Vasilyev, A. M. Vulfin, V. M. Kartak, A. D. Kirillova, and K. V. Mironov. System of attacks detection in wireless sensor networks of Industrial Internet of Things (in Russian) // Proceedings of the ISA RAS, vol. 69, no. 4, pp. 70-78, 2019. ]]

53. Вульфин А. М. Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных // Системная инженерия и информационные технологии. 2023. Т. 5. № 4 (13). С. 50–76. [[ A. M. Vulfin. Models and methods for comprehensive assessment of security risks of critical information infrastructure objects based on intelligent data analysis// System Engineering and Information Technologies. 2023. Vol. 5, No. 4 (13), pp. 50–76. ]]

*Поступила в редакцию 7 сентября 2023 г.*

**МЕТАДАННЫЕ / METADATA**

**Title:** Assessment of information security risks of automated process control systems for industrial facilities using cognitive modeling methods.

**Abstract:** A review of the results of the study of automated process control systems (APCS) of industrial facilities is presented. The subject of the research is methods, models, and algorithms for quantitative assessment of information security (IS) risks of automated process control systems for industrial facilities based on cognitive modeling methods. The purpose of the study is to increase the efficiency and reliability of risk assessment of IS risks of automated process control systems for industrial facilities using cognitive modeling technologies and machine learning methods. To achieve the goal, the following tasks are solved: 1. Analysis of the current state of the problem of providing information security for automated process control systems of industrial facilities, considering the requirements of the existing regulatory and methodological framework. 2. Development and study of a fuzzy cognitive model for quantitative risk assessment of IS ICS considering the impact of uncertainty factors and an algorithm for its construction in the class of nested gray fuzzy cognitive maps. 3. Development of a method, algorithm, and methodology

for quantitative risk assessment of IS ICS of industrial facilities based on the simulation of attack scenarios using cognitive modeling technologies and machine learning methods. 4. Development of tools for automating the simulation of scenarios of attacks on APCS as part of an intelligent decision support system (IDSS) at the stage of risk assessment of IS IS of APCS of industrial facilities. 5. Development of a methodology and practical recommendations for the application of the developed method, models, and algorithms for assessing the risks of IS APCS of industrial facilities for solving applied problems. The methods of system analysis, IS risk assessment, graph theory, cognitive modeling and machine learning were used as solution methods.

**Key words:** information security; risk assessment; cognitive modeling; fuzzy gray cognitive maps; attack scenarios.

**Язык статьи / Language:** русский / Russian.

**Об авторе / About the author:**

**КИРИЛЛОВА Анастасия Дмитриевна**
ФГБОУ ВО «Уфимский университет науки и технологий», Россия.
Ст. преп. каф. вычислительной техники и защиты информации. Дипл. преп.-исследователь. (Уфимск. гос. авиац. техн. ун-т, 2022). Канд. техн. наук по методам и системам защиты информации, инф. безопасности (Уфимск. ун-т науки и технологий, 2023). Иссл. в области обеспечения информационной безопасности.
E-mail: kirillova.andm@gmail.com
URL: https://elibrary.ru/author_profile.asp?id=1049934

**KIRILLOVA Anastasiya Dmitrievna**
Ufa University of Science and Technologies, Russia.
Senior Lecturer of the department computer technology and information security. Dipl. teacher, teacher-researcher (Ufa State Aviat. Techn. University, 2022). Cand. Tech. Sciences on methods and systems of information protection, information security (Ufa University of Science and Technology, 2023). Research in the field of information security.
E-mail: kirillova.andm@gmail.com
URL: https://elibrary.ru/author_profile.asp?id=1049934