УДК 004.056.5
DOI: 10.26102/2310-6018/2022.37.2.022

Анализ и управление рисками информационной безопасности АСУ ТП на основе когнитивного моделирования

В.И. Васильев, А.М. Вульфин✉, А.Д. Кириллова

Уфимский государственный авиационный технический университет, Уфа, Российская Федерация
vulfin.alexey@gmail.com✉

Резюме. В работе рассматривается проблема оптимизации параметров когнитивных моделей при анализе рисков информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП), отражающих оптимальное распределение затрат на реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений. Применяется генетический алгоритм оптимизации весовых коэффициентов когнитивных моделей, что позволяет определить оптимальные конфигурации мер защиты в процессе оценки рисков информационной безопасности АСУ ТП в условиях реализации сложных многошаговых атак. На примере АСУ ТП пункта сдачи-приема нефти проводится оптимизация конфигурации контрмер для выбора наиболее эффективных вариантов распределения ресурсов средств и систем защиты информации для минимизации рисков информационной безопасности. Предложенный подход позволил снизить оценку рисков информационной безопасности на 85 %, увеличить оценку эффективности эксплуатации контрмеры и уменьшить оценку стоимости эксплуатации контрмеры. Анализ соотношения полученных оценок рисков информационной безопасности в пределах выделенных зон АСУ ТП и затрат на мероприятия по их снижению позволяет определить механизмы управления защищенностью целевых ресурсов системы и поддерживать ее необходимый уровень защищенности, а также оценивать требуемые при этом затраты на интеграцию и сопровождение контрмер. Результат свидетельствует об эффективности предложенного подхода оптимизации конфигурации выбранных контрмер с учетом многокритериальной оптимизации рисков и оценкой экономических аспектов обеспечения информационной безопасности объекта.

Ключевые слова: информационная безопасность, управление рисками, нечеткие серые когнитивные карты, генетический алгоритм, контрмеры.

Благодарности: Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-38-90078.

Для цитирования: 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;10(2). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1184 DOI: 10.26102/2310-6018/2022.37.2.022

Analysis and management of ICS cybersecurity risks based on cognitive modeling

V.I. Vasilyev, A.M. Vulfin✉, A.D. Kirillova

Ufa State Aviation Technical University, Ufa, Russian Federation
vulfin.alexey@gmail.com✉

Abstract. The paper considers the problem of optimizing cognitive model parameters in the analysis of information security risks of industrial control systems (ICS), reflecting the optimal distribution of costs for the realization, implementation, and maintenance of countermeasures, taking into account their

functional limitations. A genetic algorithm for optimizing the weight coefficients of cognitive models is used, which makes it possible to determine the optimal configurations of protection measures in the process of assessing ICS information security risks under the conditions of complex multi-step attacks. On the example of the oil delivery ICS and receipt point, the optimization of the countermeasure configuration is carried out to select the most effective options for the allocation of resources of means and information security systems to minimize information security risks. The proposed approach enabled the reduction of information security risk assessment by 85%, increase the assessment of the countermeasure operating efficiency, and reduce the assessment of the countermeasure operating cost. Analysis of the correlation between the obtained information security risk assessments within the allocated ICS zones and the costs of measures to reduce them helps to determine the mechanisms for managing the security of the system target resources and maintain its required level of security as well as to assess the costs required for the integration and maintenance of countermeasures. The result testifies to the effectiveness of the proposed approach to optimizing the configuration of the selected countermeasures with due regard for the multicriteria risk optimization and assessing the economic aspects of ensuring the information security of the object.

Keywords: cybersecurity, risk management, fuzzy gray cognitive maps, genetic algorithm, countermeasures.

Acknowledgments: The reported study was funded by RFBR under the research project No. 20-38-90078.

For citation: Vasilyev V.I., Vulfin A.M., Kirillova A.D. Analysis and management of ICS cybersecurity risks based on cognitive modeling. *Modeling, Optimization and Information Technology*. 2022;10(2). Available from: https://moitvivt.ru/ru/journal/pdf?id=1184 DOI: 10.26102/2310-6018/2022.37.2.022 (In Russ.).

Введение

Сопряжение технологических и корпоративных сегментов сетевой инфраструктуры предприятий, наличие связи между различными зонами сети, а также развитие механизмов удаленного обслуживания создают предпосылки для возникновения угроз информационной безопасности (ИБ) автоматизированной системы управления технологическими процессами (АСУ ТП) и предприятия в целом [1, 2].

В настоящее время нет общепринятого подхода для выбора оптимального набора средств защиты информации и оценки эффективности их применения для конкретной сети и перечня актуальных угроз. Кроме того, построение любой системы защиты информации должно начинаться с анализа рисков ИБ. Каждый риск после оценки подлежит анализу для выбора меры работы с ним: минимизация, принятие, уклонение, перевод и диверсификация [3]. Необходим выбор инструмента управления для каждого риска и оценка их эффективности применения.

Ключевой задачей становится совершенствование методик для обеспечения поддержки принятия решений по выбору наиболее эффективного набора контрмер.

В [4] разработана методика количественной оценки рисков ИБ на основе технологий когнитивного моделирования и Text Mining, расширяющая возможности Методики оценки угроз безопасности информации ФСТЭК России [5]. Предложенный в работе подход основан на построении семантической модели дескрипторов ИБ объектов информационной системы и позволяет автоматизировать процесс моделирования сценариев реализации угроз на основе описания шаблонов компьютерных атак, содержащихся в базах данных (БДУ ФСТЭК, NVD, MITRE), характеризующих различные аспекты безопасности программного и аппаратного обеспечения инфраструктуры сети промышленных объектов.

Предлагается при анализе рисков ИБ АСУ ТП решать задачу оптимизации параметров когнитивных моделей, отражающих оптимальное распределение затрат на

реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений.

Нечеткие серые когнитивные карты в задаче оценки рисков ИБ АСУ ТП

Количественная оценка рисков ИБ АСУ ТП в [4] реализуется на основе нечетких серых когнитивных карт (НСКК). Важным преимуществом когнитивной модели является возможность формализации численно неизмеримых факторов, использование неполной, нечеткой и противоречивой информации и возможности учета разброса мнений экспертов.

НСКК оценки рисков ИБ определяется в виде ориентированного графа, заданного с помощью кортежа множеств:

$$\text{НСКК} = \{C, E, W\},$$

где $C = \{C_i\}$ – множество концептов (вершин графа), $(i = 1, 2, ..., n)$; $E = \{E_{ij}\}$ – множество связей между концептами (дуг графа); $W = \{W_{ij}\}$ – множество весов связей, $(i, j) \in \Omega$. Здесь $\Omega = \{(i_1, j_1), (i_2, j_2), ..., (i_S, j_S)\}$ – множество пар индексов смежных (т. е. связанных между собой) вершин графа, $S \le n(n-1)$.

Веса связей НСКК и состояния концептов задаются с помощью «серых» (интервальных) чисел $\otimes W_{ij}$, определяемых как $\otimes W_{ij} \in [\underline{W}_{ij}, \overline{W}_{ij}]$, где $\underline{W}_{ij} < \overline{W}_{ij}$, $\{\underline{W}_{ij}, \overline{W}_{ij}\} \in [-1,1]$, $\underline{W}_{ij}$ и $\overline{W}_{ij}$ – соответственно нижняя и верхняя границы 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 $[\underline{W}_{ij}, \overline{W}_{ij}] \in [-1,1]$.

В [1] предлагается формализация семантической модели дескрипторов безопасности объектов в виде иерархической НСКК (Рисунок 1), позволяющей анализировать сценарии реализации атак с требуемым уровнем детализации за счет механизмов декомпозиции и укрупнения [6].

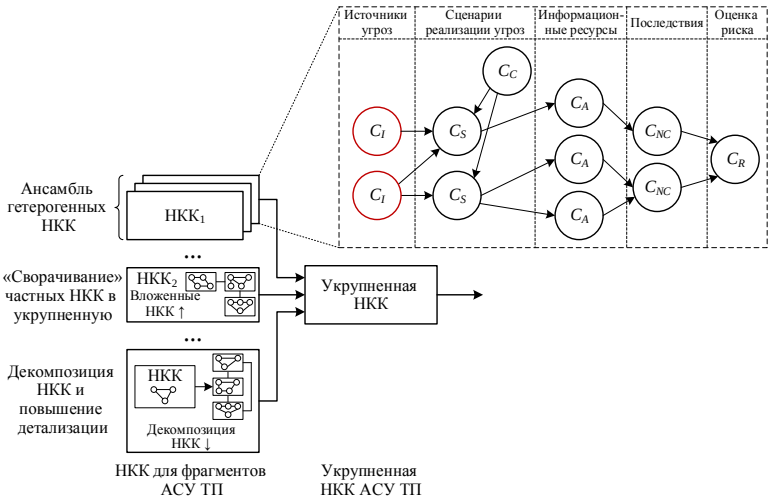


Рисунок 1 – Иерархическая НСКК для оценки рисков ИБ АСУ ТП
Figure 1 – Hierarchical FGCM for ICS information security risk assessment

На Рисунке 1: C_I – определение источников угроз; C_S – определение способов реализации угроз по средствам эксплуатации уязвимостей (сценарий = тактики + техники); C_A – определение компонент и информационных ресурсов; C_{NC} – определение негативных последствий для промышленной системы; C_C – выбор рационального способа защиты с учетом ограничений; C_R – оценка риска.

Каждая атака укрупняется до концепта НСКК с соответствующими весовыми коэффициентами, позволяющими оценить вероятность реализации атаки в каждом из возможных сценариев. Результирующая НСКК позволяет оценить уровень локальных относительных рисков при реализации воздействия злоумышленника на промышленную систему. Наиболее детализированный уровень НСКК отражает ряд действий злоумышленника на каждом этапе реализации атаки, что позволяет получить развернутую итоговую оценку локального относительного риска ИБ для целевых объектов промышленной системы. Под локальным относительным риском R_i понимается потенциальный ущерб, наносимый i-му активу АСУ ТП предприятия (в относительных единицах) и приводящей к определенным киберфизическим последствиям.

Однако недостатком предложенной методики является высокий уровень требований к компетенциям специалиста по ИБ и фрагментарная поддержка основных этапов методики вспомогательным программным обеспечением для моделирования атак и оценки уязвимостей.

Оценка эффективности распределения ресурсов контрмер

Нечеткие когнитивные карты являются удобным средством для представления знаний экспертов, однако трудности возникают при определении большого количества весов связей между концептами НСКК при решении задач многокритериальной оптимизации с ограничениями оценок рисков ИБ при моделировании сценариев применения контрмер.

Будем полагать, что целью моделирования с помощью НСКК является анализ эффективности распределения ресурсов применяемых контрмер (Рисунок 2), а также оценка особенностей их интеграции в существующую информационную систему организации и последующее сопровождение на всех этапах жизненного цикла.

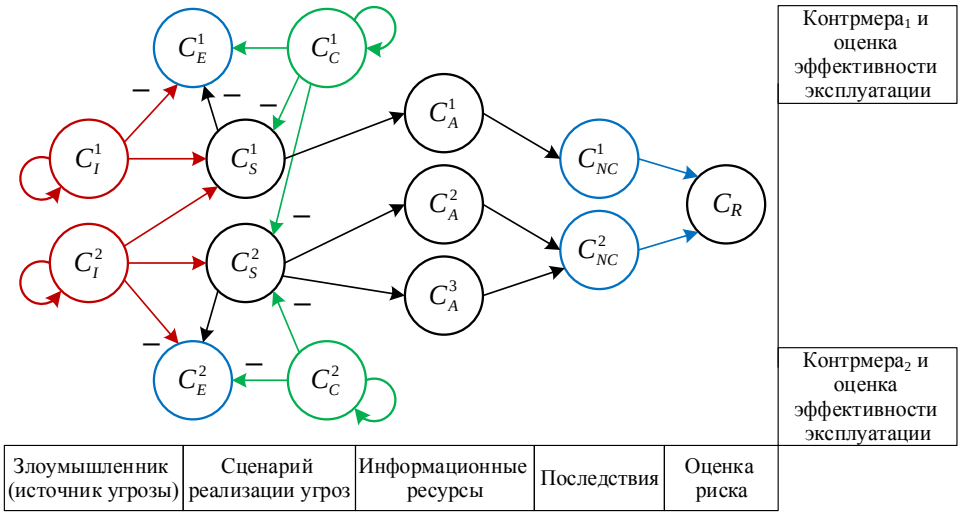


Рисунок 2 – НСКК для оценки эффективности распределения ресурсов контрмер
Figure 2 – FGCM for assessing the effectiveness of countermeasure resource allocation

Значение концепта C_R НСКК на Рисунке 2 определяет итоговую оценку X_R относительного риска ИБ для моделируемых сценариев 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 контрмер C_C^1 и C_C^2 при моделировании сценариев реализации угроз ИБ. Установившиеся значения концептов C_E^1 и C_E^2 позволяют оценить эффективность интеграции и использования каждой контрмеры.

Таким образом, возможна следующая формальная постановка задачи оптимизации:

$$\Phi\left(W_{C_C^i,C_S^j}\right) = X_R \to \min,$$

где $\Phi(\cdot)$ – целевая функция, X_R – установившееся значение концепта C_R, $W_{C_C^i,C_S^j}$ – настраиваемые параметры, характеризующие распределение ограниченных ресурсов контрмеры C_C^i для снижения вероятности реализации сценариев угроз C_S^j.

На параметры $W_{C_C^i,C_S^j}$ накладывается ряд условий (1), связанных со спецификой определения весов в базисе «серых» чисел:

$$\forall W_{C_C^i,C_S^j}: \begin{cases} \overline{W}_{C_C^i,C_S^j}, \underline{W}_{C_C^i,C_S^j} \in [0;1] \\ \overline{W}_{C_C^i,C_S^j} > \underline{W}_{C_C^i,C_S^j} \\ \sum_i \left[\overline{W}_{C_C^i,C_S^j} + \underline{W}_{C_C^i,C_S^j}\right] < \theta \end{cases} \quad (1)$$

Для применения классических реализаций алгоритмов оптимизации с ограничениями целевую функцию представим как норму вектора компонент серого числа X_R с дополнительным заданием штрафной компоненты (2), обеспечивающей корректное определение области значений $\overline{X}_R, \underline{X}_R \in [0;1]$:

$$\Phi\left(W_{C_C^i,C_S^j}\right) = \left\|\overline{X}_R, \underline{X}_R\right\| + \alpha f\left(\overline{X}_R, \underline{X}_R\right), \qquad f\left(\overline{X}_R, \underline{X}_R\right) = \begin{cases} 1, \overline{X}_R < 0, \underline{X}_R < 0 \\ 0, \text{otherwise} \end{cases}. \quad (2)$$

Для оптимизации весовых коэффициентов когнитивной карты возможно использовать генетический алгоритм (ГА) [7-9], относящийся к классу стохастических алгоритмов поиска субоптимального решения с нелинейными ограничениями [10, 11] и области задания, и области значения целевой функции.

Анализ соотношения полученных оценок рисков ИБ и затрат на мероприятия по их снижению позволяет определить механизмы управления защищенностью целевых ресурсов системы и поддерживать ее необходимый уровень, а также оценивать требуемые при этом затраты на интеграцию и сопровождение контрмер. В результате работы ГА будет получен набор весовых коэффициентов НСКК, отражающих оптимальное распределение затрат на реализацию мер по снижению рисков ИБ АСУ ТП.

Применение ГА позволяет формулировать задачу многокритериальной оптимизации, например, в следующей постановке (3):

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

$$\Phi\left(W_{C_C^i,C_S^j}\right)=\left\|\overline{X}_R,\underline{X}_R\right\|+\sum\nolimits_i\left\|\overline{X}_C^i,\underline{X}_C^j\right\|+\alpha f\left(\overline{X}_R,\underline{X}_R\right)+\beta f\left(\overline{X}_C^i,\underline{X}_C^j\right), \quad (3)$$

учитывающей одновременную минимизацию и оценки рисков, и суммарной оценки эффективности использования контрмер в различных сценариях моделирования.

Пример оценки рисков ИБ АСУ ТП с многокритериальной оптимизацией весов НСКК с помощью генетического алгоритма

В качестве объекта защиты рассмотрим фрагмент базовой модели территориально распределенной системы – АСУ ТП пункта сдачи приема нефти (АСУ ТП ПСП) (Рисунок 3).

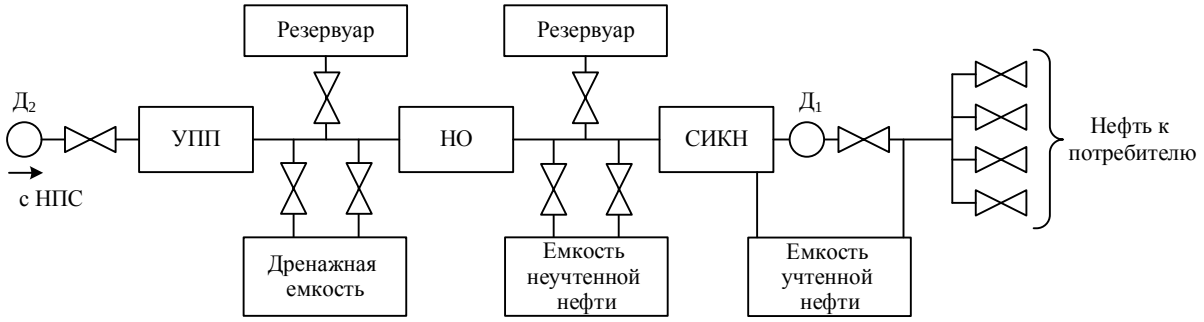


Рисунок 3 – Базовая модель АСУ ТП ПСП ($Д_1$ – датчики СИКН; $Д_2$ – датчики на входе НПС; УПП – установка подогрева продукта; НО – насосное оборудование; НПС – нефтеперекачивающая станция)

Figure 3 – Base model of an ICS for an oil delivery point (S_1 – OQMS sensors; S_2 – sensors at the intel of the OPS; PHU – product heating unit; PE – pumping equipment; OPS – oil pumping station; OQMS – oil quantity measuring system).

АСУ ТП ПСП в системе магистральных трубопроводов предназначена для автоматизации управления и оперативного контроля технологического процесса, включая сбор данных о технологических параметрах процесса: расход, уровень, температура, давление, плотность и влажность перекачиваемой нефти.

Подсистемы АСУ ТП ПСП согласно терминологии ГОСТ 62443 можно рассматривать как отдельные зоны безопасности, объединяемые по общим показателям риска, функциональным и/или техническим характеристикам, логическим или физическим границам, сетям передачи данных и т. д. На Рисунке 4 представлено зонирование по принципу единства выполняемых функций и требований к безопасности их реализации:

- зона 1 – зона сервера СДКУ (система диспетчерского контроля и управления) SCADA;
- зона 2 – зона критических устройств управления;
- зона 3 – зона управления задвижками;
- зона 4 – зона управления ТП ПСП;
- зона 5 – зона управления системой измерения количества нефти (СИКН);
- зона 6 – зона датчиков.

В [4] построена модель угроз для Зоны 5 с помощью разработанной методики оценки рисков ИБ АСУ ТП. Были выявлены наиболее критичные ресурсы рассматриваемого объекта: промышленная сеть предприятия, промышленный коммутатор и программируемый логический контроллер (ПЛК).

Разработано ПО для автоматизированной оценки рисков ИБ [12] и последующего анализа риска для подбора контрмер, минимизирующих выявленный уровень риска, на языке программирования высокого уровня C#. Моделирование сценариев реализации угроз и эксплуатации уязвимостей реализовано на основе построения семантической модели отношений между дескрипторами CVE, BDU, CWE, CAPEC объектов [13], а также построения НСКК с оптимизацией весов посредством применения ГА.

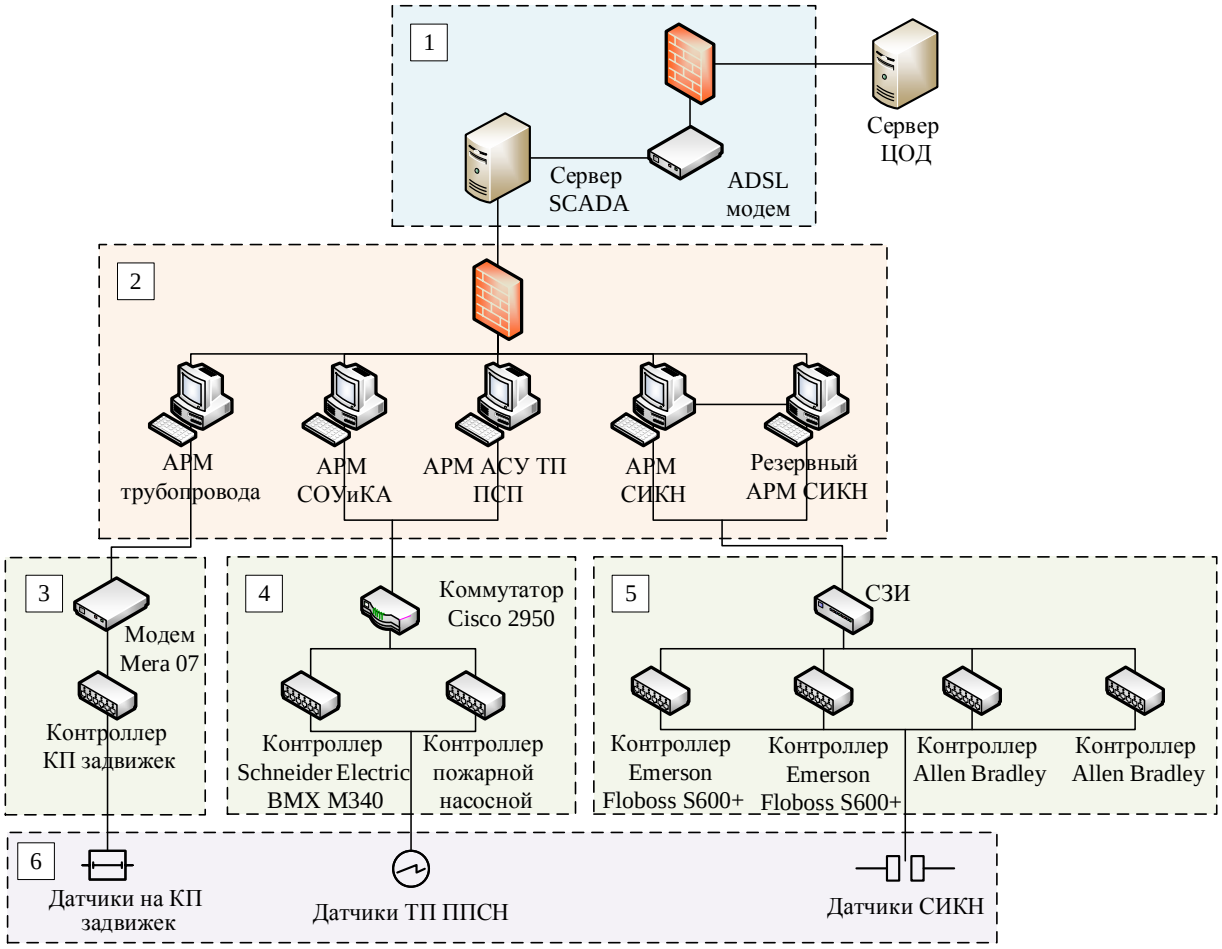


Рисунок 4 – Зональная модель объекта защиты
Figure 4 – Zone model of the protected object

Разработанное ПО обеспечивает:

– поддержку принятия решений при работе с открытыми базами угроз, уязвимостей и шаблонов атак (CVE, BDU, CWE, CAPEC), что позволяет специалистам по ИБ, зная конкретные уязвимости рассматриваемого объекта, получить наглядную графовую модель [14, 15];

– формализацию семантической модели в виде иерархической НСКК, позволяющей анализировать сценарии атак с требуемым уровнем детализации и оптимизацией весовых коэффициентов НСКК при помощи ГА для распределения ресурсов контрмер.

С помощью разработанного ПО выполним поиск по ключевым фразам из описания объектов системы и для сужения области поиска воспользуемся следующими идентификаторами CWE IDs:

– 798 – Use of Hard-coded Credentials (использование жестко заданных учетных данных) – обход проверки подлинности настроенного администратором ПО;

– 287 – Improper Authentication (неправильная аутентификация);
– 863 – Incorrect Authorization (неправильная авторизация).

Список уязвимостей, наиболее подходящий под модель рассматриваемого объекта, приведен в Таблице 1.

Таблица 1 – Список уязвимостей на основе анализа объекта защиты
Table 1 – List of vulnerabilities based on analysis of the protected object

Уязвимость	Описание
CVE-2019-6859	В контроллерах Modicon существует уязвимость CWE-798: использование жестко закодированных учетных данных, что может привести к раскрытию жестко закодированных учетных данных FTP при использовании веб-сервера контроллера в незащищенной сети.
CVE-2019-6812	Уязвимость CWE-798, связанная с использованием жестко закодированных учетных данных, существует в BMX-NOR-0200H с версиями прошивки до V1.7 IR 19, что может вызвать проблемы с конфиденциальностью при использовании протокола FTP.
CVE-2020-7507	В Easergy T300 (версия микропрограммы 1.5.2 и старше) существует уязвимость CWE-400: неконтролируемое потребление ресурсов, которая может позволить злоумышленнику войти в систему несколько раз, что приведет к отказу в обслуживании.
BDU:2020-01893	Уязвимость микропрограммного обеспечения оборудования Modicon Controllers, связана с наличием жестко закодированных учетных данных, используемых для передачи конфигурационных файлов оборудованию Modicon Controllers. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольную команду в отношении оборудования Modicon Controllers.
BDU:2020-04014	Уязвимость микропрограммного обеспечения логического контроллера Modicon M218 Logic Controller связана с записью за границы буфера памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.
BDU:2019-03754	Уязвимость микропрограммного обеспечения программируемых логических контроллеров Allen Bradley компании Rockwell Automation связана с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код в результате использования модифицированного встроенного программного обеспечения.
CVE-2018-19616	Проблема была обнаружена в Rockwell Automation Allen-Bradley PowerMonitor 1000. Неаутентифицированный пользователь может добавлять / редактировать / удалять администраторов, поскольку контроль доступа реализован на стороне клиента через атрибут disabled для элемента BUTTON.

Для списка уязвимостей выполняется подбор шаблонов эксплуатации уязвимостей и реализации угроз ИБ АСУ ТП [4, 6] с помощью разработанного ПО [12] (Рисунок 5).

Список найденных связей от CWE к CAPEC

Cwe	CAPEC
CWE-798	Capec-70
CWE-200	Capec-116, Capec-13, Capec-169, Capec-22, Capec-224, Capec-508
CWE-287	Capec-114, Capec-115, Capec-151, Capec-194, Capec-22, Capec-94

Список найденных связей от CAPEC к ATTACK/OWASP/WASC

CapecId	Taxonomies
Capec-70	ATTACK Id 1078,001, ATTACK Id 1110,003
Capec-13	ATTACK Id 1562,003, ATTACK Id 1574,006, ATTACK Id 1574,007
Capec-169	ATTACK Id 1217
Capec-224	WASC Id 45
Capec-194	WASC Id 38
Capec-94	ATTACK Id 1185

Рисунок 5 – Список шаблонов атак, которые могут быть реализованы через выявленные уязвимости
Figure 5 – List of attack patterns that can be implemented through identified vulnerabilities

Итоговая семантическая модель, сформированная в автоматизированном режиме и описывающая взаимосвязь уязвимостей, угроз и сценариев их реализации для рассматриваемого объекта, приведена на Рисунке 6.

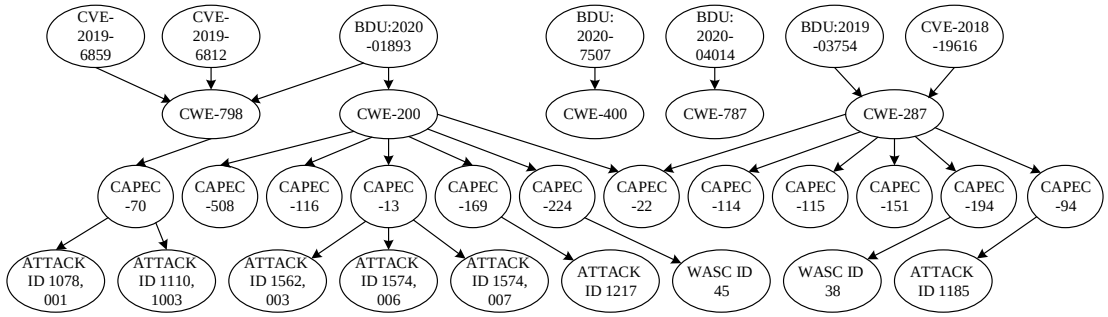


Рисунок 6 – Графовая модель, описывающая взаимосвязь уязвимостей, угроз и сценариев их реализации
Figure 6 – Graph model describing the relationship of vulnerabilities, threats, and scenarios for their implementation

С учетом построенной графовой модели реализации сценариев атак и модели угроз объекта строятся актуальные способы эксплуатации уязвимостей и реализации угроз для зоны 5 АСУ ТП ПСП в виде НСКК. Итоговая цепочка действий злоумышленника в виде укрупненной НСКК$_1$ представлена на Рисунке 7. Концепты для моделирования НСКК$_1$ приведены в Таблице 2.

Таблица 2 – Концепты НСКК$_1$ для моделирования актуальных способов реализации угроз
Table 2 – FGCM$_1$ concepts for modeling current methods of threat implementation

Концепт	Характеристика
C_1	Злоумышленник, реализующий сетевую атаку
C_2	Подмена ответа сервера FTP резервного копирования конфигураций ПЛК (УБИ.034)
C_3	Перехват учетной записи привилегированного пользователя на ПЛК (УБИ.034)
C_4	Учетная запись с параметрами по умолчанию на ПЛК (УБИ.030)

Таблица 2 (продолжение)
Table 2 (continued)

C_5	Модификация прошивки ПЛК (УБИ.188)
C_6	Перезапись проекта ПЛК в режиме online (УБИ.179)
C_7	Отказ в обслуживании оборудования
C_8	Потеря возможности мониторинга параметров СИКН
C_9	Перевод СИКН и управляемых объектов в аварийное состояние
C_{10}	Останов нефтетранспорта по магистральному нефтепроводу
C_{11}	Нарушение штатного режима функционирования АСУ ТП ПСП
C_{12}	Неспособность компании выполнить договорные обязательства
C_{13}	Система обнаружения аномалий сетевого трафика и мониторинга состояния компонент ИС и хода ТП
C_{14}	Оценка затрат на реализацию мер по снижению риска ИБ
C_{15}	Оценка эффективности применения СЗИ

Концепт C_1 выступает в качестве концепта-драйвера и представляет собой внешнего злоумышленника, реализующего сетевую атаку, связанную с модификацией конфигураций ПЛК с целью нарушения ТП, создания аварийной ситуации на промышленном объекте или состояния аварийной остановки. Также в качестве концепта-драйвера установлен C_{13} – система обнаружения аномалий сетевого трафика и мониторинга состояния ресурсов АСУ ТП и хода ТП [16-19], т. е. предлагаемая контрмера для минимизации рисков ИБ АСУ ТП. Фиксированным значением концепта-драйвера является оценка вероятности обнаружения аномалий состояния информационно-телекоммуникационной сети и наблюдаемого объекта, полученные в [19].

Целевыми установлены концепты-последствия C_{11} и C_{12}. Установившееся значение концепта C_{15} характеризует оценку эффективности применения контрмер. Нормированная в диапазон [0; 1] оценка затрат на реализацию мер по снижению рисков ИБ характеризуется состоянием концепта C_{14}.

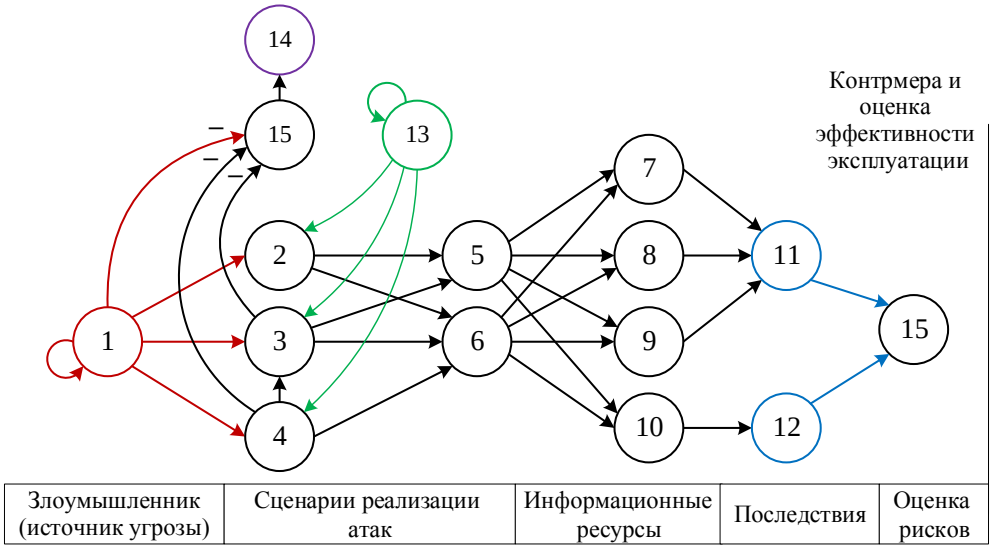


Рисунок 7 – Визуализация НСКК$_1$
Figure 7 – FGCM$_1$ visualization

Целевая функция для НСКК$_1$:

$$X_{11}, X_{12} \to \min; \qquad \Phi\left(W_{13,C_S^j}\right) = X_{11}, X_{12} \to \min, \ j = 2,3,4.$$

Применяемая контрмера обладает ограниченными возможностями оперативного анализа входящего сетевого трафика и трафика внутри промышленной сети без существенных задержек. Следовательно, необходимо распределение ресурсов ($W_{13,2}$, $W_{13,3}$, $W_{13,4}$, суммарное пороговое значение распределяемых ресурсов $\theta \le 3$) контрмеры для анализа трафика между наиболее значимыми объектами АСУ ТП с целью минимизации итогового суммарного ущерба. Значение концепта-драйвера C_{13} задается оценкой эффективности обнаружения аномалий сетевого трафика и состояния объекта $X_{13} = [0,95; 0,98]$.

На область определения целевой функции $\Phi\left(W_{13,C_S^j}\right)$ наложены следующие ограничения:

$$\forall W_{13,i}: \begin{cases} \overline{W}_{13,i}, \underline{W}_{13,i} \in [0,05; 0,95], \ i = 2,3,4; \\ \overline{W}_{13,i} - \underline{W}_{13,i} \ge 0,05; \\ \sum\left[\overline{W}_{13,i} + \underline{W}_{13,i}\right] < 3. \end{cases}$$

Целевая функция с заданными ограничениями на область значений:

$$\Phi\left(W_{13,i}\right) = \left\|\underline{X}_{11}, \overline{X}_{11}, \underline{X}_{12}, \overline{X}_{12}\right\| + \alpha f\left(\underline{X}_{11}, \overline{X}_{11}, \underline{X}_{12}, \overline{X}_{12}\right);$$

$$f\left(\underline{X}_{11}, \overline{X}_{11}, \underline{X}_{12}, \overline{X}_{12}\right) = \begin{cases} 1, X_j < \varepsilon; \\ 0, \text{otherwise.} \end{cases} \qquad \varepsilon = 1e-4; \ j = \overline{1,4}.$$

Определим перечень характеристик интеграции и последующего сопровождения контрмер для рассматриваемой промышленной системы (Таблица 3) и декомпозируем концепт C_{14} в соответствии с выделенными особенностями (Рисунок 8) для уточнения итоговой оценки эффективности решения.

Таблица 3 – Концепты НСКК$_2$ декомпозиции концепта C_{14} НСКК$_1$
Table 3 –FGCM$_2$. concepts of C_{14} FGCM$_1$ concept decomposition

Концепт	Характеристика
C_1	Стоимость контрмер
C_2	Простота эксплуатации и сопровождения
C_3	Стоимость сопровождения контрмер
C_4	Степень влияния на штатное функционирование
C_5	Импортозамещение
C_6	Оперативность реагирования контрмер
C_7	Концепт C_{15} от НСКК$_1$
C_8	Концепт C_{14} от НСКК$_1$

Значение концептов вложенной НСКК$_2$ определяется после стабилизации состояния концептов НСКК$_1$ согласно схеме [6].

Для оценки локального относительного риска рассмотрим следующие сценарии моделирования.

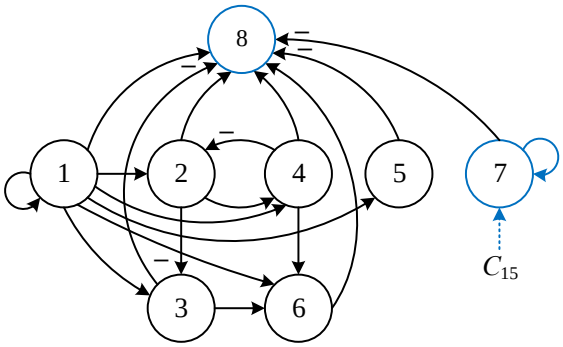
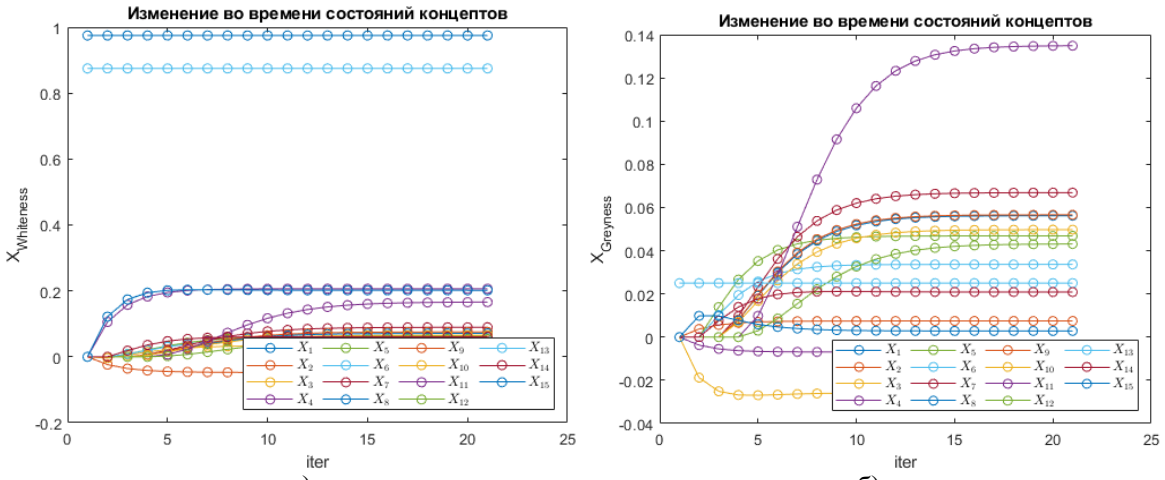


Рисунок 8 – Декомпозиция концепта C_{14}
Figure 8 – Decomposition of C_{14} concept

Сценарий 1. Изменение во времени концептов НСКК$_1$ без оптимизации распределения весовых коэффициентов контрмеры C_{13}. Процесс изменения состояний концептов НСКК$_1$ во времени показан на Рисунке 9, где по оси ординат отмечены значения переменных состояния концептов НСКК$_1$, а по оси абсцисс – итерации сходимости НСКК$_1$.

Итоговые значения целевых концептов НСКК$_1$: $X_{11} = [0,03; 0,3]$ и $X_{12} = [0,01; 0,10]$, а также $X_{15} = [0,2; 0,2]$.

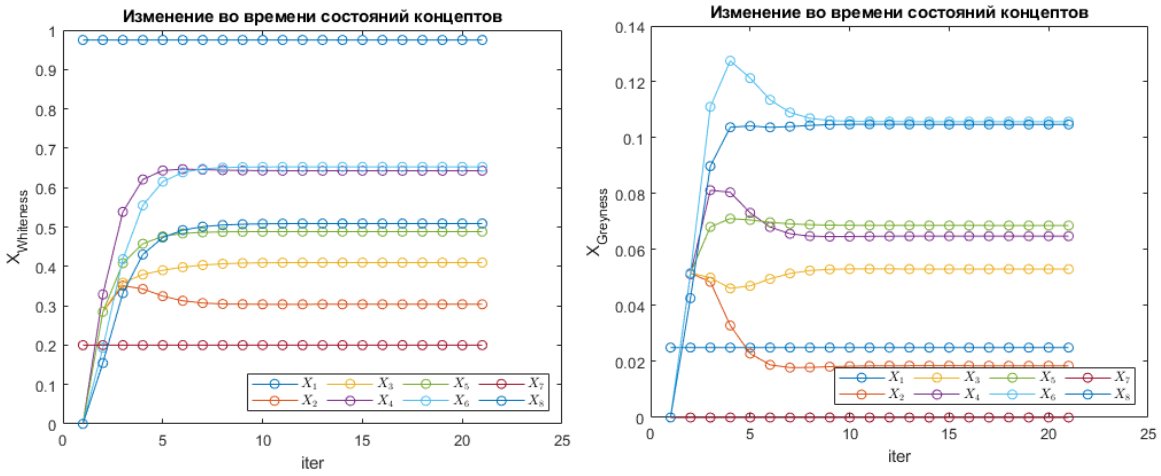


а) б)

Рисунок 9 – Стабилизация состояния концептов НСКК$_1$: а) «белизна» и б) «серость» оценок состояния концептов
Figure 9 – Stabilization of FGCM$_1$ concept states: a) “whiteness” and b) “greyness” of concept state assessment

Изменение во времени состояния концептов вложенной НСКК$_2$ без оптимизации распределения весовых коэффициентов контрмеры C_{13} представлено на Рисунке 10.

Итоговое значение целевого концепта НСКК$_2$ составило $X_8 = [0,4; 0,61]$.



а) б)

Рисунок 10 – Стабилизация состояния концептов НСКК$_2$: а) «белизна» и б) «серость» оценок состояния концептов

Figure 10 – Stabilization of FGCM$_2$ concept state: a) “whiteness” and b) “greyness” of concept state assessment

Сценарий 2. Рассмотрим применение ГА для оптимизации весовых коэффициентов $W_{13,2}$, $W_{13,3}$, $W_{13,4}$. Размер начальной популяции составляет 100 особей. Изменение среднего значения фитнес-функции по популяции и значения фитнес-функции для лучшей особи в популяции по итерациям ГА приведено на Рисунке 11.

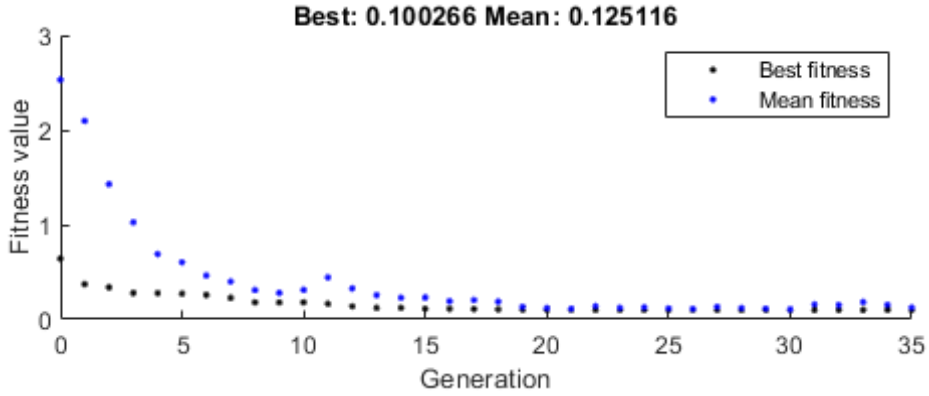
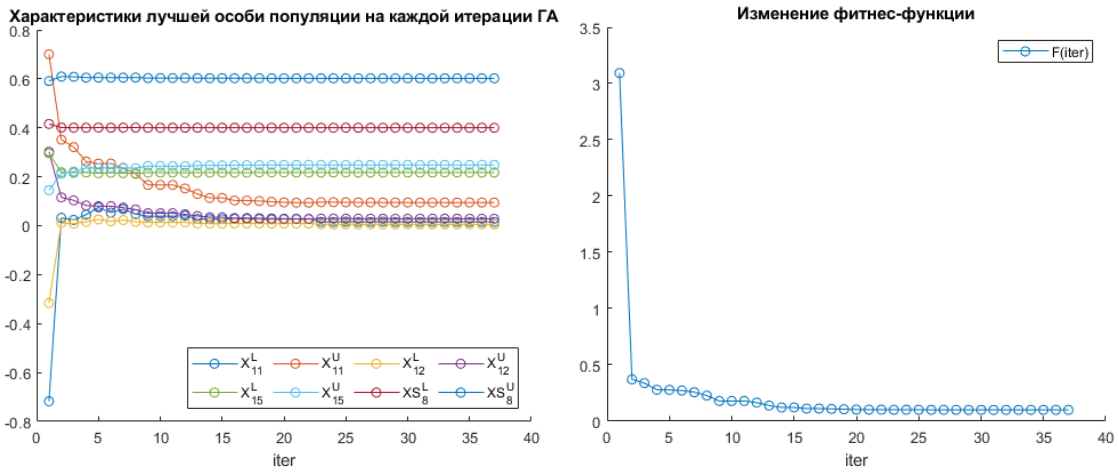


Рисунок 11 – Изменение среднего значения фитнес-функции по популяции и значения фитнес-функции для лучшей особи в популяции по итерациям ГА

Figure 11 – Changes in the average value of the fitness function by population and the values of the fitness function for the best individual in the population by GA iterations

Изменение во времени значений целевых концептов НСКК$_1$ – X_{11}, X_{12} и мониторинг состояния концепта X_8 для НСКК$_2$ по итерациям ГА показаны на Рисунке 12.

Значение параметров по результатам оптимизации для НСКК$_1$ – $X_{11} = [0,0153; 0,0947]$, $X_{12} = [0,0054; 0,0287]$, $X_{15} = [0,2175; 0,2486]$, для НСКК$_2$ – $X_8 = [0,4003; 0,6025]$. Значение фитнес-функции – 0,1003.



а) б)

Рисунок 12 – а) изменение во времени значений целевых концептов НСКК$_1$ – X_{11}, X_{12} и концепта X_8 для НСКК$_2$ по итерациям ГА; б) изменение фитнес-функции по итерациям ГА
Figure 12 – a) changes in the time of the target concept values FGCM$_1$ – X_{11}, X_{12} and X_8 concept for FGCM$_2$ by iterations of the GA; b) changes of fitness function by GA iterations

Изменение подбираемых весовых коэффициентов, характеризующих распределение контрмер, по итерациям работы ГА показано на Рисунке 13.

Итоговые значения целевых концептов НСКК$_1$ составили: $X_{11} = [0,03; 0,03]$ и $X_{12} = [0,01; 0,10]$, а также концепта $X_{15} = [0,2; 0,2]$.

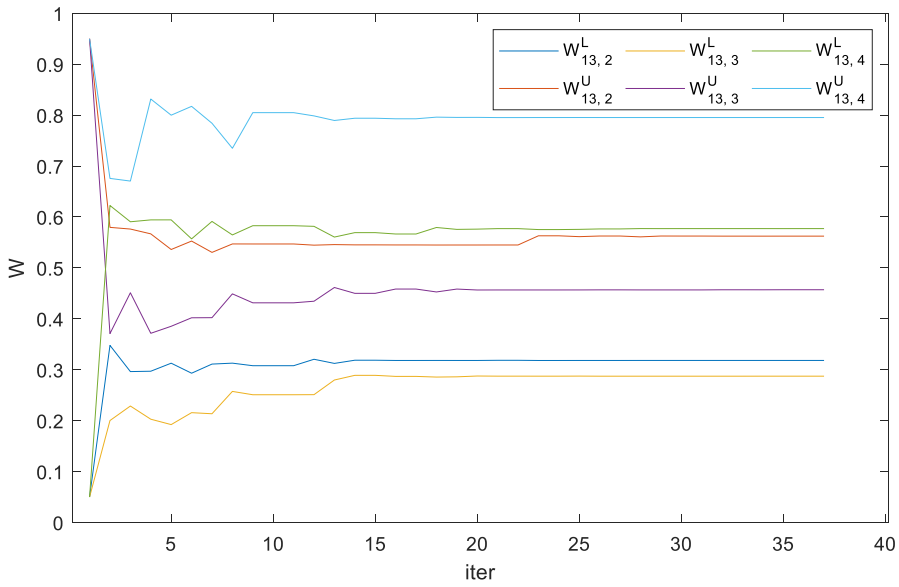


Рисунок 13 – Изменение подбираемых весовых коэффициентов по итерациям работы ГА
Figure 13 – Changes in the selected weight coefficients by iterations of the GA operation

Итоговая диаграмма состояний целевых концептов НСКК$_1$ и НСКК$_2$ приведена на Рисунке 14.

Анализ диаграммы показывает, что оценки локального относительного риска ИБ для целевых концептов C_{11} и C_{12} после оптимизации распределения ресурсов контрмеры уменьшились как в отношении разброса («серость»), так и в отношении центрального значения оценок («белизна») на 85-90 %. Отметим, что возросла оценка эффективности

эксплуатации контрмеры (состояние концепта X_{15}) и уменьшилась оценка стоимости эксплуатации контрмеры несмотря на то, что в целевую функцию оптимизация этих параметров заложена не была. Следовательно, предложенный подход демонстрирует эффективность в выборе наиболее эффективных вариантов средств защиты при минимальных затратах и позволяет оптимизировать распределение ресурсов системы защиты информации для минимизации рисков ИБ.

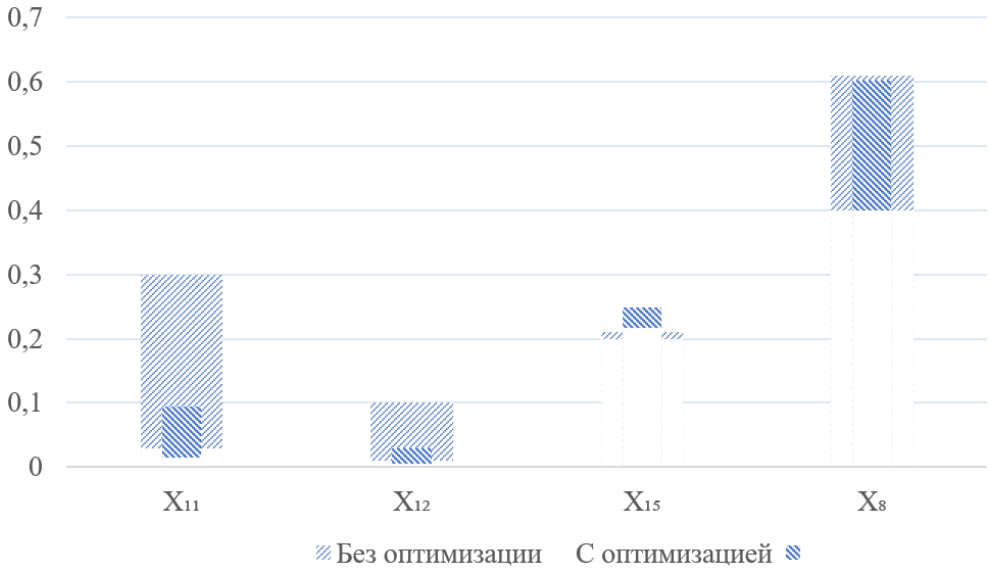


Рисунок 14 – Состояние целевых концептов НСКК$_1$ и НСКК$_2$ (по оси ординат – диапазон значения серых оценок состояния концептов)
Figure 14 – The state of FGCM$_1$ and FGCM$_2$ target concepts (on the ordinate –the range of concept state gray assessment values)

Заключение

Построение когнитивной модели обеспечивает детализированную оценку рисков ИБ АСУ ТП, что делает выбор контрмер более обоснованным. И поскольку исходными данными для построения НСКК являются не только экспертные оценки, но и формализованные и систематизированные данные из открытых баз угроз и уязвимостей, существенно повышается обоснованность и полнота моделирования.

Применение генетического алгоритма оптимизации весовых коэффициентов НСКК позволяет определить оптимальные конфигурации мер защиты в процессе оценки рисков ИБ АСУ ТП в условиях реализации сложных многошаговых атак. В рассматриваемом примере проведена оптимизация конфигурации выбранных контрмер с учетом многокритериальной оптимизации рисков и оценкой экономических аспектов обеспечения ИБ объекта.

СПИСОК ИСТОЧНИКОВ

1. Зегжда Д.П. и др. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации. *Вопросы кибербезопасности*. 2018;2(26):2–14.
2. Alshamrani A. et al. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*. 2019;2(21):1851–1877.
3. Машкина И.В. Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий: дис.… д-ра техн.

наук. *Уфа: Изд-во ГОУ ВПО Уфимский государственный авиационный технический университет*. 2009.
4. 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;3:110–134. DOI: 10.24412/2410-9916-2021-3-110-134 (ВАК)
5. Методика оценки угроз безопасности информации. Методический документ ФСТЭК России от 5 февраля 2021 г. Официальный сайт ФСТЭК России Доступно по: https://fstec.ru/component/attachments/download/2919 (дата обращения: 13.05.2022).
6. Васильев В.И., Кириллова А.Д., Вульфин А.М. Когнитивное моделирование вектора кибератак на основе меташаблонов CAPEC. *Вопросы кибербезопасности*. 2021;2(42):2–16.
7. Jamshidi A. et al. Dynamic risk assessment of complex systems using FCM. *International Journal of Production Research*. 2018;56(3):1070–1088.
8. Haritha K., Judy M.V. Fuzzy cognitive map-based genetic algorithm for community detection. *Progress in advanced computing and intelligent engineering. Springer, Singapore.* 2021:412–426.
9. Salmeron J.L. et al. Learning fuzzy cognitive maps with modified asexual reproduction optimisation algorithm. *Knowledge-Based Systems*. 2019;163:723–735.
10. Sivanandam S.N., Deepa S.N. Genetic algorithm optimization problems. *Introduction to genetic algorithms. Springer, Berlin, Heidelberg*. 2008:165–209.
11. Padmalatha E. et al. Feature Selection Optimization Using a Hybrid Genetic Algorithm. *ICT Analysis and Applications. Springer, Singapore.* 2021:411–421.
12. Кириллова А.Д., Вульфин А.М., Ягафаров Р.Р., Васильев В.И., Зиязетдинова Л.Ю. Свидетельство о государственной регистрации программы для ЭВМ № 2021619894 Российская Федерация. Программа анализа и моделирования кибератак на основе меташаблонов в нечетком когнитивном базисе: заявл. 07.06.2021; опубл. 18.06.2021.
13. Богданов Ю.М., Огарок А.Л., Селиванов С.А. Мониторинг кибербезопасности сложных информационных и управляющих систем критической инфраструктуры. *Информатизация и связь*. 2021;1:142–150.
14. Bakhtavar E. et al. Fuzzy cognitive maps in systems risk analysis: a comprehensive review. *Complex & Intelligent Systems*. 2021;7(2):621–637.
15. Amirkhani A., Nasiriyan-Rad H., Papageorgiou E.I. A novel fuzzy inference approach: neuro-fuzzy cognitive map. *International Journal of Fuzzy Systems*. 2020;22(3):859–872.
16. Selivanov S.A., Ogarok A.L. Providing cybersecurity of complex information and control systems. *Informatization and Communication*. 2020;1:28–33.
17. Arpishkin M.I. et al. Intelligent integrity monitoring system for technological process data. *Journal of Physics: Conference Series. IOP Publishing*. 2019;1368(5):052029.
18. Vulfin A.M., Vasilyev V.I., Kirillova A.D., Nikonov A.V. Cognitive security modeling of biometric system of neural network cryptography. *Proceedings of the Information Technologies and Intelligent Decision Making Systems (ITIDMS2021). CEUR*. 2021;2843.
19. Vulfin A.M., Vasilyev V.I., Kuharev S.N., Homutov E.V., Kirillova A.D. Algorithms for detecting network attacks in an enterprise industrial network based on data mining algorithms. *International Scientific and Practical Conference "Information Technologies and Intelligent Decision Making Systems (ITIDMS-II 2021). Journal of Physics: Conference Series.* 2021;2001:012004.

REFERENCES

1. Zegzhda D.P. et al. Advanced production technologes security in the era of digital

transformation. *Voprosy kiberbezopasnosti*. 2018;2(26):2–14. (In Russ.)
2. Alshamrani A. et al. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*. 2019;2(21):1851–1877.
3. Mashkina I.V. Information security management in the segment of the corporate information system based on intelligent technologies: dis.… dr. tech. sciences. *Ufa: Publishing house of GOU VPO Ufa State Aviation Technical University*. 2009. (In Russ.)
4. Vasilyev V.I., Vulfin A.M., Kirillova A.D., Kuchkarova N.V. Methodology for assessing current threats and vulnerabilities based on cognitive modeling technologies and Text Mining. *Systems of Control, Communication and Security*. 2021;3:110–134. (In Russ.)
5. Methodology for assessing information security risks. FSTEC of Russia, 2021 URL: https://fstec.ru/component/attachments/download/2919 (accessed on 13.05.2022) (In Russ.)
6. Vasilyev V.I., Kirillova A.D., Vulfin A.M. Cognitive modeling of the cyber attack vector based on CAPEC methods. *Voprosy kiberbezopasnosti*. 2021;2(42):2–16. (In Russ.)
7. Jamshidi A et al. Dynamic risk assessment of complex systems using FCM. *International Journal of Production Research*, vol. 2018;56(3):1070–1088.
8. Haritha K., Judy M.V. Fuzzy cognitive map-based genetic algorithm for community detection. *Progress in advanced computing and intelligent engineering. Springer, Singapore*. 2021:412–426.
9. Salmeron J.L. et al. Learning fuzzy cognitive maps with modified asexual reproduction optimisation algorithm. *Knowledge-Based Systems*. 2019;163:723–735.
10. Sivanandam S.N., Deepa S.N. Genetic algorithm optimization problems. *Introduction to genetic algorithms. Springer, Berlin, Heidelberg*. 2008:165–209.
11. Padmalatha E. et al. Feature Selection Optimization Using a Hybrid Genetic Algorithm. *ICT Analysis and Applications. Springer, Singapore*. 2021:411–421.
12. Kirillova A.D., Vulfin A.M., Yagafarov R.R. and Vasiliev V.I., Ziyazetdinova L.Yu. Certificate of state registration of a computer program No. 2021619894 Russian Federation. Program for the analysis and modeling of cyberattacks based on meta-templates in a fuzzy cognitive basis: Appl. 06/07/2021; publ. 06/18/2021. (In Russ.)
13. Bogdanov Y.M., Ogarok A.L., Selivanov S.M. Monitoring cybersecurity of complex information and control systems of critical infrastructure. *Informatizaciya i svyaz'*. 2021;1:142–150. (In Russ.)
14. Bakhtavar E. et al. Fuzzy cognitive maps in systems risk analysis: a comprehensive review. *Complex & Intelligent Systems*. 2021;7(2):621–637.
15. Amirkhani A., Nasiriyan-Rad H., Papageorgiou E.I. A novel fuzzy inference approach: neuro-fuzzy cognitive map. *International Journal of Fuzzy Systems*. 2020;22(3):859–872.
16. Selivanov S.A., Ogarok A.L. Providing cybersecurity of complex information and control systems. *Informatization and Communication*. 2020;1:28–33.
17. Arpishkin M.I. et al. Intelligent integrity monitoring system for technological process data. *Journal of Physics: Conference Series. IOP Publishing*. 2019;1368(5):052029.
18. Vulfin A.M., Vasilyev V.I., Kirillova A.D., Nikonov A.V. Cognitive security modeling of biometric system of neural network cryptography. *Proceedings of the Information Technologies and Intelligent Decision Making Systems (ITIDMS2021). CEUR*. 2021;2843.
19. Vulfin A.M., Vasilyev V.I., Kuharev S.N., Homutov E.V., Kirillova A.D. Algorithms for detecting network attacks in an enterprise industrial network based on data mining algorithms. *International Scientific and Practical Conference "Information Technologies and Intelligent Decision Making Systems (ITIDMS-II 2021). Journal of Physics: Conference Series*. 2021;2001:012004.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Васильев Владимир Иванович, доктор технических наук, профессор Уфимского государственного авиационного технического университета, Уфа, Российская Федерация.
e-mail: vasilyev@ugatu.ac.ru

Vladimir Ivanovich Vasilyev, Doctor of Technical Science, Professor of Ufa State Aviation Technical University, Ufa, Russian Federation.

Вульфин Алексей Михайлович, кандидат технических наук, доцент Уфимского государственного авиационного технического университета, Уфа, Российская Федерация.
e-mail: vulfin.alexey@gmail.com
ORCID: 0000-0001-5857-2413

Alexey Mikhailovich Vulfin, Candidate of Technical Sciences, Associate Professor of Ufa State Aviation Technical University, Ufa, Russian Federation.

Кириллова Анастасия Дмитриевна, аспирант, ассистент Уфимского государственного авиационного технического университета, Уфа, Российская Федерация.
e-mail: kirillova.andm@gmail.com

Anastasia Dmitrievna Kirillova, Postgraduate Student, Assistant of Ufa State Aviation Technical University, Ufa, Russian Federation.

Статья поступила в редакцию 15.05.2022; одобрена после рецензирования 07.06.2022; принята к публикации 28.06.2022.

The article was submitted 15.05.2022; approved after reviewing 07.06.2022; accepted for publication 28.06.2022.