Научная статья
УДК 004.056.5; 004.822; DOI: 10.61260/2218-13X-2024-3-86-97

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ И НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ

✉Паршенкова Юлия Анатольевна;
Максимова Елена Александровна.
МИРЭА – Российский технологический университет, Москва, Россия.
Матвеев Александр Владимирович.
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉parshenkova@mirea.ru

Аннотация. Рассматривается применение нейронных сетей и нечетких когнитивных карт для анализа рисков информационной безопасности на объектах критической информационной инфраструктуры. Авторы исследуют возможности использования этих методов для оценки и прогнозирования потенциальных рисков, а также рассматриваются подходы к адаптации этих технологий под конкретные условия и требования безопасности. В ходе исследования в качестве базовой использовалась методология когнитивного моделирования. Особое внимание уделяется анализу эффективности и точности предложенных методов, а также их применимости в реальных условиях эксплуатации информационных систем. Результаты работы включают в себя исследование модели оценки рисков информационной безопасности на основе нейронных сетей и нечетких когнитивных карт, а также рекомендации по применению данной модели для повышения уровня защищенности объектов критической информационной инфраструктуры. Практическая значимость данного исследования заключается в более точной оценке рисков и, как следствие, принятию наиболее рациональных шагов для их снижения.

Ключевые слова: информационная безопасность, критическая информационная инфраструктура, риски информационной безопасности, угрозы информационной безопасности, нейронная сеть, когнитивные карты

Для цитирования: Паршенкова Ю.А., Максимова Е.А., Матвеев А.В. Анализ рисков информационной безопасности на объектах критической информационной инфраструктуры с помощью нейронных сетей и нечетких когнитивных карт // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 3. С. 86–97. DOI: 10.61260/2218-13X-2024-3-86-97.

Scientific article

ANALYSIS OF INFORMATION SECURITY RISKS AT CRITICAL INFORMATION INFRASTRUCTURE FACILITIES USING NEURAL NETWORKS AND FUZZY COGNITIVE MAPS

✉Parshenkova Yuliya A.;
Maksimova Elena A.
MIREA – Russian technological university, Moscow, Russia.
Matveev Alexander V.
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉parshenkova@mirea.ru

Abstract. The article discusses the use of neural networks and fuzzy cognitive maps to analyze information security risks at critical information infrastructure facilities. The authors explore

the possibilities of using these methods to assess and predict potential risks, and also consider approaches to adapting these technologies to specific conditions and safety requirements. In the course of the study, the methodology of cognitive modeling was used as a basic one. Special attention is paid to the analysis of the effectiveness and accuracy of the proposed methods, as well as their applicability in real-world operating conditions of information systems. The results of the work include a study of an information security risk assessment model based on neural networks and fuzzy cognitive maps, as well as recommendations on the use of this model to increase the level of security of critical information infrastructure facilities. The practical significance of this study lies in a more accurate assessment of risks and, as a result, taking the most rational steps to reduce them.

Keywords: information security, critical information infrastructure, information security risks, information security threats, neural network, cognitive maps

For citation: Parshenkova Yu.A., Maksimova E.A., Matveev A.V. Analysis of information security risks at critical information infrastructure facilities using neural networks and fuzzy cognitive maps // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 3. P. 86–97. DOI: 10.61260/2218-13X-2024-3-86-97.

Введение

Автоматизированные системы управления технологическими процессами (АСУ ТП) являются базой, лежащей в основе циклов производства на объектах критической информационной инфраструктуры (КИИ).

С учетом нестабильной геополитической обстановки за последние три года резко возросло число успешных атак, направленных на компьютеры АСУ.

Так, по сообщению Kaspersky ICS CERT [1], за первые четыре месяца в России вредоносное программное обеспечение (ПО) было найдено и нейтрализовано на 23,6 % компьютеров АСУ. Неутешительными являются данные о том, что некоторые среднемировые показатели в России превышены. Ярким подтверждением являются данные по количеству компьютеров промышленного назначения, являющихся носителями вредоносного ПО.

Например, в строительстве он составил 24,2 % против 23,7 % в мире, а в инжиниринге и среди интеграторов АСУ – 27,2 % против 24 % [1]. В России особенно заметен тренд, когда злоумышленники активно атакуют интеграторов, доверенных партнёров и подрядчиков. Это указывает на серьёзность сложившейся ситуации и необходимость принять срочные меры для её улучшения.

На сегодняшний день ключевым направлением деятельности российских специалистов является работа по усовершенствованию законодательной базы для обеспечения безопасности в киберпространстве компьютеров АСУ ТП на субъектах КИИ. Главной целью в данном вопросе выступает обеспечение непрерывности и целостности самого технологического процесса. Стоит отметить, что имеющиеся нормативные документы основаны на методологии системного риск-ориентированного подхода к обеспечению кибербезопасности АСУ ТП. Эта методология имеет много общего с методологией когнитивного моделирования, получившей широкую популярность за последние несколько лет. Суть последней состоит в построении и последующем анализе нечётких когнитивных карт (Fuzzy Cognitive Maps, FCM). За их основу взяты знания и опыт экспертов-специалистов в рассматриваемом вопросе.

Анализ и оценка рисков информационной безопасности на объектах КИИ

За последний год резко выросло число кибератак на российские информационные ресурсы. Очевидно, что наибольший интерес для злоумышленников представляют значимые объекты КИИ, так как урон, причиненный им, связан с наибольшими потерями. Так, согласно

информации, предоставленной Федеральной службой безопасности Российской Федерации, с начала 2024 г. было зафиксировано более четырех тысяч хакерских атак на объекты КИИ [2]. Этот всплеск активности сделал выполнение требований Федерального закона от 26 июля 2017 г. № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» ещё более актуальным. Кроме того, всё больше специалистов интересуются средствами и методами защиты КИИ и способами их эффективного применения, вне зависимости от того, предусмотрена ли ответственность за несоблюдение требований по их использованию или нет. Обозначенное не только определяет актуальность и приоритетность вопросов обеспечения безопасности значимых объектов КИИ, но и должно быть отражено в моделях оценки рисков информационной безопасности (ИБ) КИИ. Оценка рисков ИБ может определяться как на количественном, так и на качественном уровнях и должна быть соотнесена с требуемым уровнем ИБ.

Минимальный порог защищенности для объекта, которому необходима защита, называют базовым уровнем защищенности [3]. Базовый уровень защищенности не только помогает предотвратить наиболее часто встречающиеся угрозы, но и является основой для дальнейшего увеличения уровня ИБ объекта. Стоит отметить, что в разных странах для данного уровня существуют разные критерии [4]. Обозначенное рассматривается в рамках базового анализа рисков, выполняемого с учетом требований базового уровня защищенности. Методы данного анализа, как правило, не учитывают ценность объекта, а производят исключительно оценку мер защиты. Применение подобных методов целесообразно только в тех случаях, когда к объекту не применимы высокие требования защищенности.

Для обеспечения безопасности систем на должном уровне требуется проведение комплексного анализа возможных рисков. В него входит не только выявление вредоносного воздействия и противостояние ему, но и выбор наиболее рациональных мер по устранению такого воздействия. Помимо этого, затраты на защиту объекта также должны учитываться в ходе проведения проактивного анализа данных, направленного на минимизацию риска с помощью внедрения средств защиты, устранение риска путем выведения из работы атакованных ресурсов, перекладывания возмещения ущерба на страховую компанию или принятие риска [5]. Схема реализации обозначенного представлена на рис. 1.

При проведении анализа в обязательном порядке производится оценка потенциального ущерба, и рассчитывается вероятность успешного стороннего вмешательства в работу объекта КИИ [6]. При расчете понесенного урона учитывается стоимость объекта КИИ, а также степень тяжести последствий от нарушения его работы. Для того чтобы степень была определена наиболее корректно, проводят анализ всех важных свойств объекта, подвергшегося вмешательству.

К примеру, нарушение конфиденциальности может нанести ущерб репутации организации и утечке данных в открытые источники, что приведет к финансовым проблемам из-за судебных исков партнеров и клиентов [7].

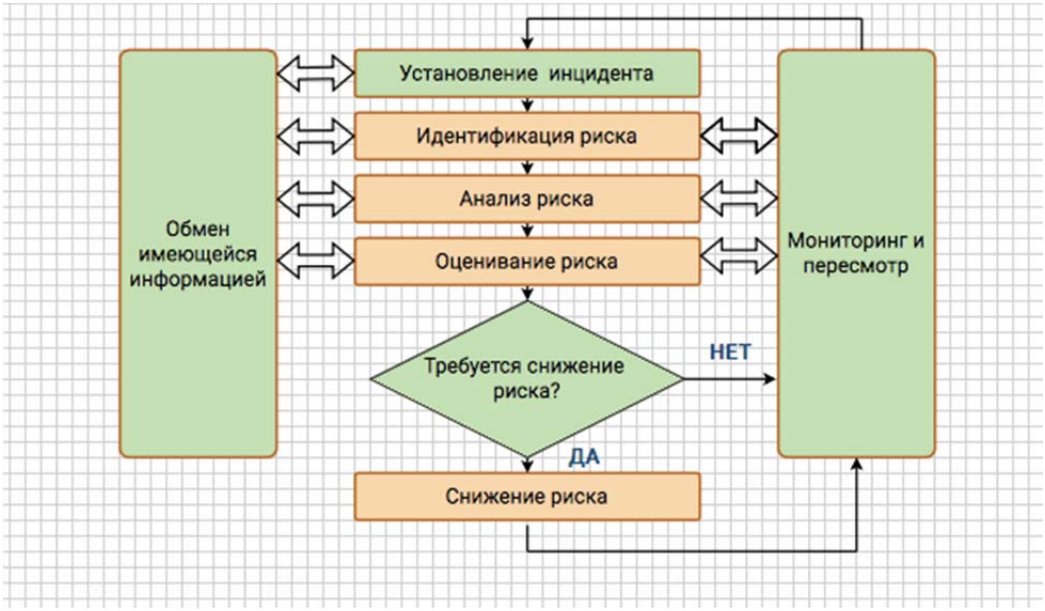

Рис. 1. **Схема реализации процедуры анализа и оценка рисков ИБ**

Нарушение целостности может привести к искажению или полному уничтожению данных, что вызовет необходимость их восстановления.

Нарушение доступности может привести к временной или постоянной недоступности информационных ресурсов, что приведет к простою в работе.

Общая оценка тяжести последствий нарушения безопасности объектов КИИ учитывает все вышеперечисленные аспекты. Эта оценка позволяет определить величину риска и разработать соответствующие меры по его снижению [8].

Анализ рисков ИБ обязательно включает в себя оценку вероятности реализации угроз. Она позволяет определить, насколько вероятно то или иное негативное событие, связанное с нарушением безопасности активов предприятия. Вероятность реализации угрозы может быть оценена различными способами, в зависимости от характера угрозы и доступных данных [9]. При расчете вероятности атаки могут быть использованы данные статистики за последний период времени, построение сценариев атаки и пр. При грамотном расчете возможного ущерба и вероятности возникновения стороннего вмешательства удастся более точно вычислить степень риска, который представляет собой комбинацию потенциально причиненного ущерба и вероятность возникновения несанкционированного вмешательства.

Для наиболее точного вычисления риска применяют так называемую матрицу рисков. Строки матрицы представляют собой потенциальные значения причиненного ущерба, а в столбцах указывается степень вероятности успешной реализации несанкционированного воздействия. На пересечении выбранных показателей расположена величина риска. Неоспоримым преимуществом матрицы является ее наглядность, что позволяет принять решение по возникшему риску наиболее точно и рационально.

Сравнивая рассчитанные уровни риска с рабочей шкалой, можно выполнить оценку реального влияния этих рисков на деятельность предприятия. Стоит отметить, что в ходе оценивания рисков должна осуществляться идентификация на предмет приемлемых уровней риска с целью выявления ситуаций, в процессе которых дальнейшие действия не потребуются. Во всех остальных случаях дополнительные меры по защите безопасности являются необходимыми [10].

По результатам оценки определяется целесообразность проведения тех или иных действий по обеспечению безопасности, причем это касается не только применяемых мер защиты объекта, но и экономической составляющей [11].

Считается, что сама идея управления рисками берет свое начало с разработки модели безопасности Клементса-Хоффмана, но стоит заметить, что в процессе работы с ней появилась необходимость проведения оценки угроз ИБ. Суть рассматриваемой модели заключается в том, что на каждый сценарий несанкционированного воздействия у системы, обеспечивающей безопасность, обязательно должно быть средство защиты. Иными словами, должны быть предусмотрены все угрозы и потенциальные уязвимости.

Для описания системы защиты информации с полным перекрытием рассматривается схема организации рисков ИБ (рис. 2).

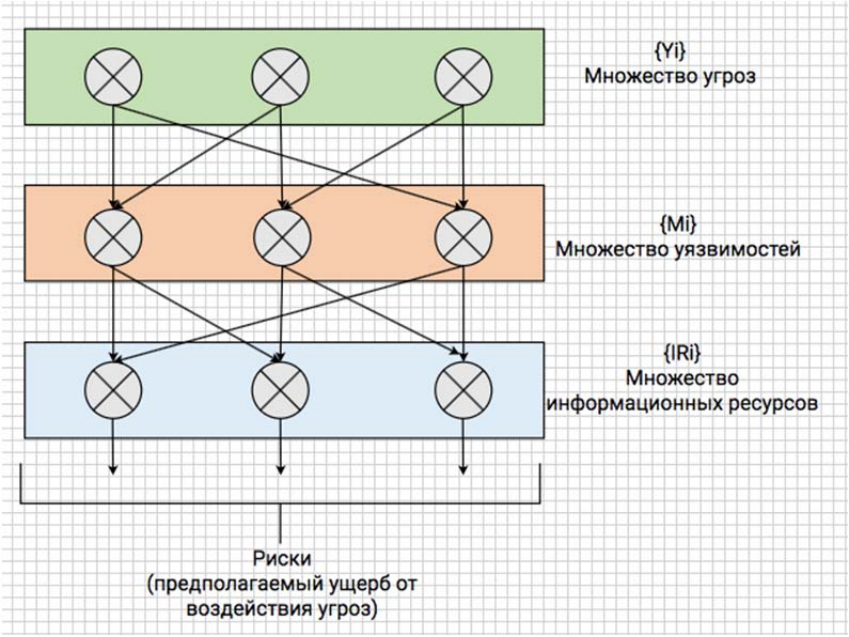

Рис. 2. **Общая схема формирования рисков ИБ (модель Клементса-Хоффмана)**

Формулу для расчета риска ИБ можно представить в виде [5]:

РИСК=УГРОЗА * УЯЗВИМОСТЬ * ИНФОРМАЦИОННЫЙ РЕСУРС.

Локальный риск (для *i*-го информационного ресурса):

$$R_i=f(P_{угрi},P_{уязвi},C_{ИРi}),$$

где $R_i=C_{ущi}/C_{ИРi}$; $P_{угрi}$ и $P_{уязвi}$, – вероятности появления *i*-й угрозы и реализации *i*-й уязвимости; $C_{ИРi}$ – стоимость (ценность) *i*-го информационного ресурса (ИР); $C_{ущi}$ – величина ущерба от реализации *i*-й угрозы [5].

Для совокупности информационных ресурсов:

а) максимальный локальный риск:

$$R_{imax}=\max\{R_i\}\ (1\le i\le n);$$

б) общий (суммарный) риск:

$$R_\Sigma=\Sigma_{i=1}^{n} a_i R_i,$$

где $a_i=C_{ИРi}/C_{ИР\Sigma}$ – удельный вес (значимость) *i*-го ИР; $C_{ИРi}=\Sigma_{i=1}^{n} C_{ИРi}$ – общая стоимость (ценность) всех ИР.

Схематическое представление оценки общего риска представлено на рис. 3.

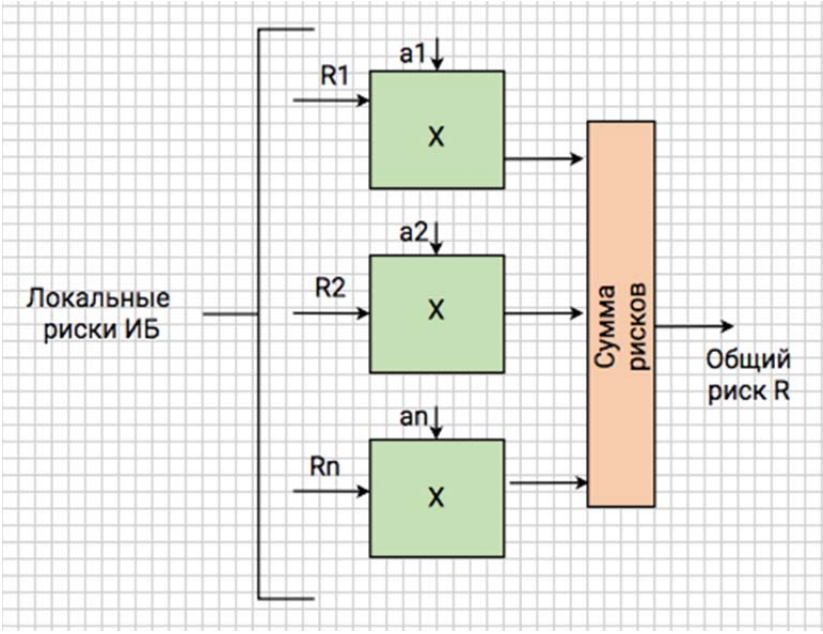

Рис. 3. **Вычисление общего риска ИБ**

Система защиты информации должна строиться с учетом степени защиты объекта от несанкционированного воздействия. Чтобы достичь наибольшей эффективности, угрозы следует сортировать в соответствии со степенью опасности и мерами, применяемыми по их обработке. Это позволит оптимизировать решения в системе управления ИБ [12, 13].

Нейронные сети как средство анализа рисков ИБ

В основе реализации нейронных сетей заложены математические модели организации биологических нейронных сетей. Анализ рисков ИБ с помощью нейронных сетей представляет собой мощный инструмент для выявления потенциальных угроз и уязвимостей ИБ. Нейронные сети обладают способностью обучаться на значительных объёмах данных и определять сложные паттерны, что было бы невозможно сделать с использованием традиционных методов анализа. Применение нейронных сетей для анализа рисков ИБ имеет ряд преимуществ:

1) высокая точность. Нейронные сети способны обрабатывать большие объёмы данных и выявлять сложные закономерности, что позволяет им обеспечивать высокую точность анализа;

2) автоматизация процесса. Нейронные сети могут автоматизировать процесс анализа рисков, что позволяет сократить время и ресурсы, затрачиваемые на этот процесс;

3) адаптивность. Нейронные сети могут адаптироваться к изменениям в окружающей среде, что делает их эффективным инструментом для анализа рисков ИБ.

Процесс анализа рисков ИБ с помощью нейронных сетей включает несколько ключевых этапов:

1) сбор данных: на этом этапе происходит сбор данных, необходимых для обучения нейронной сети. Данные могут включать информацию о предыдущих инцидентах ИБ, характеристиках систем и сетей, а также о внешних факторах, влияющих на безопасность. Нейронные сети могут анализировать сетевой трафик, активность программ и поведение пользователей, выявляя необычное поведение, которое может свидетельствовать о кибератаках;

2) подготовка данных: собранные данные проходят предварительную обработку, включающую очистку, нормализацию и преобразование в формат, подходящий для обучения нейронной сети;

3) выбор архитектуры нейронной сети в соответствии с поставленными задачами;

4) процесс обучения нейронной сети на базе имеющихся данных;

5) тестирование и валидация: после обучения проводится тестирование нейронной сети на новых данных, не использованных в процессе обучения. Это позволяет оценить точность и надежность предсказаний нейронной сети;

6) интерпретация результатов: результаты работы нейронной сети анализируются для выявления потенциальных рисков ИБ. Контекстно это может быть представлено анализом выявленных аномалий в поведении систем, результатом мониторинговых процедур, связанных с поиском уязвимостей и оценки вероятности реализации угроз;

7) принятие мер по снижению рисков: полученные данные используются в решении управленческих задач по оптимизации используемых ресурсов и системы защиты информации. Это может включать обновление ПО, усиление мер аутентификации и авторизации, а также внедрение дополнительных средств защиты;

8) проведение мониторинга: по завершению внедрения мер, применяемых в ходе снижения рисков, продолжается мониторинг состояния ИБ. В случае обнаружения новых угроз или изменения условий эксплуатации системы, нейронная сеть может быть дообучена для адаптации к новым условиям. Этот процесс позволяет использовать преимущества нейронных сетей для эффективного анализа рисков ИБ и принятия обоснованных решений по их снижению [14].

Однако использование нейронных сетей для анализа рисков ИБ также имеет ряд недостатков:

1) сложность настройки. Настройка нейронной сети требует глубоких знаний в области машинного обучения и искусственного интеллекта;

2) необходимость больших объёмов данных. Для обучения нейронной сети требуется большое количество данных, что может быть затруднительно в некоторых случаях;

3) риск переобучения. Нейронные сети могут переобучаться, то есть запоминать обучающие данные вместо выявления закономерностей.

Также использование нейронных сетей в кибербезопасности сопряжено с рядом проблем и вызовов, таких как возможность обмана нейронных сетей злоумышленниками, недостаток данных для обучения и необходимость защиты самих нейронных сетей от атак. Несмотря на эти недостатки, нейронные сети являются перспективным инструментом для анализа рисков ИБ. Они могут использоваться для выявления потенциальных угроз, оценки вероятности их реализации и определения мер по их предотвращению.

Но для наиболее эффективного использования нейронных сетей в анализе рисков ИБ необходимо сочетать их с другими методами и инструментами кибербезопасности, такими как системы обнаружения вторжений, мониторинг безопасности, а также применение методов и технологий нечеткого когнитивного моделирования [15].

Использование нечетких когнитивных карт оценке рисков ИБ

Нечеткая когнитивная карта (Fuzzy Cognitive Map) представляет собой модель в форме ориентированного графа:

$$НКК = <C, F, W>,$$

где $C=\{C_i\}$ – множество концептов (вершин графа); $F=\{F_{ij}\}$ – множество связей между концептами (дуг графа); $W=\{W_{ij}\}$ – множество весов связей; i, j,..n; n – число вершин графа [16].

Для определения значимости взаимосвязей между концептами применяют нечеткие отношения, которые задаются на шкале от 0 до 1. Эти отношения могут быть выражены через лингвистические значения или представлены числовыми значениями на той же шкале. В рамках данной задачи веса отражают степень уязвимости элементов сетевой топологии.

К примеру, для нечеткой модели, концепты которой описаны в табл. 1, необходимо оценить риски нарушения конфиденциальности (C_5) и целостности (C_6) информации,

вызванные попыткой несанкционированного доступа (НСД) (C_1) и воздействием вредоносного ПО (C_2) (рис. 4).

Таблица 1

Концепты когнитивной модели

№ концептов	Наименование концептов	Переменные состояния, Xi
C1	Попытка НСД к информации	Вероятность возникновения воздействия
C2	Результат антропоморфизма межобъектного взаимодействия (АМВ) [16]	Вероятность возникновения воздействия
C3	База данных, имеющаяся на сервере	Часть утраченных или искаженных записей, к общему количеству
C4	Электронный документооборот предприятия	Часть времени на простои или восстановление нормальной работы к общему времени
C5	Ущерб вследствие нарушения конфиденциальности информации	Величина ущерба, в отн. ед.
C6	Ущерб вследствие нарушения целостности информации	Величина ущерба, в отн. ед.
C7	Контрмеры по защите информации (ЗИ)	Стоимость контрмер, в отн. ед.

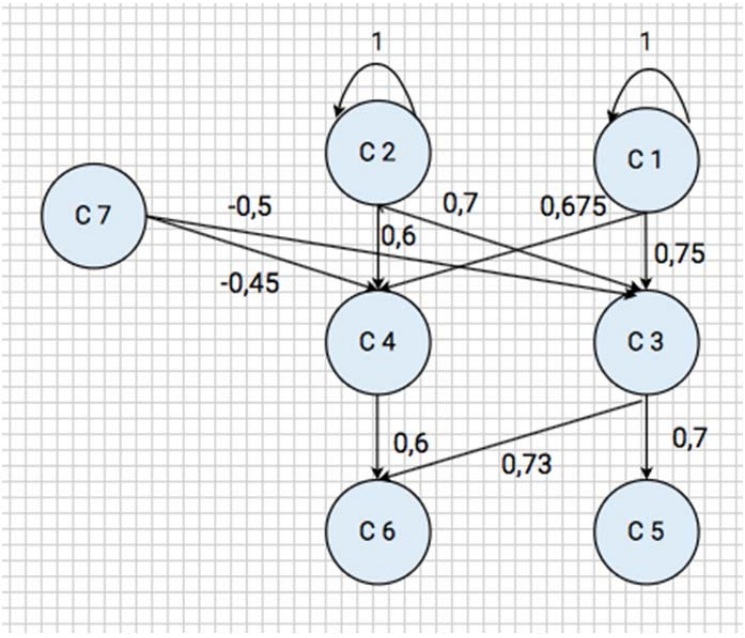

Рис. 4. **Пример когнитивной карты оценки рисков ИБ, связанных с попытками НСД и воздействием вредоносного ПО**

В данном случае рассматриваем следующие сценарии развития событий:

Сценарий A – НСД при отсутствии контрмер по ЗИ: X(0)=(0.9,0,0,0,0,0,0).

Сценарий B – результат антропоморфизма межобъектного взаимодействия при отсутствии контрмер по ЗИ: X(0)=(0.9,0,0,0,0,0,0).

Сценарий C – НСД при использовании контрмер по ЗИ: X(0)=(0.9,0,0,0,0,0,0.9).

Сценарий D – результат антропоморфизма межобъектного взаимодействия при использовании контрмер по ЗИ: X(0)=(0,0.9,0,0,0,0.9).

В ходе реализации динамического моделирования получены следующие данные (рис. 5, табл. 2).

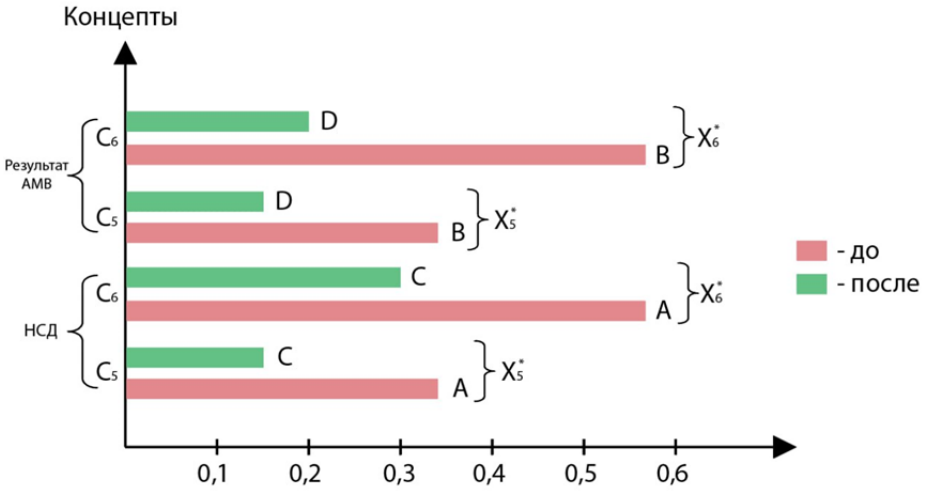

Рис. 5. **Риски ИБ до и после принятия контрмер по ЗИ**

Таблица 2

Риски ИБ до и после принятия контрмер по ЗИ

Риски ИБ	НСД		Вредоносное ПО	
	до принятия контрмер	после принятия контрмер	до принятия контрмер	после принятия контрмер
Нарушение конфиденциальности	0,34	0,135	0,325	0,12
Нарушение целостности	0,555	0,25	0,53	0,195

Примечание: значения переменных со штрихом – это установившиеся значения переменных X_5, X_6 (через 8–10 итераций)

Заключение

Неоспоримым преимуществом использования нечетких когнитивных карт в ходе проведения оценки рисков ИБ является их способность не только работать с неопределённостью и нечёткостью данных, но и с разными уровнями вероятности возникновения рисков и их степенью влияния на ИБ. Возможность адаптации и совершенствования карт с учетом требований к ИБ также является плюсом. Но в данном методе присутствуют и недостатки. При работе с нечеткими когнитивными картами

необходима оценка взаимосвязей между концептами. Как правило, оценка проводится экспертами, что может повлечь за собой субъективность и сделать более сложным процесс оценки при увеличении числа факторов. Как альтернатива, предлагается использовать нейронные сети, обучив их самостоятельно оценивать взаимосвязи. Конечно, выдаваемые нейронными сетями результаты могут зависеть от множества факторов, что затруднит определить итоговый результат, но преодолеть эту сложность можно при помощи применения искусственных нейронных сетей, анализирующих как общие, так и специфические параметры в качестве исходных данных, основываясь на методах и стандартах, принятых в стране использования. В исследованиях отмечается, что искусственные нейронные сети могут аппроксимировать любую непрерывную функцию с требуемой точностью. Однако на данный момент не существует конструктивного подхода, который гарантировал бы создание нейронных сетей с заранее заданными свойствами, что ограничивает их применение.

Список источников

1. Региональные системы. Инжиниринговый центр: Волгоград. URL: https://www.ec-rs.ru/blog/novosti/ataki-na-avtomatizirovannye-sistemy-upravleniya-tekhnologicheskimi-protsessam/ (дата обращения: 21.06.2024).

2. Федеральная служба безопасности Российской Федерации. URL: http://www.fsb.ru/fsb/press.htm (дата обращения: 21.06.2024).

3. Максимова Е.А. Оценка информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях. Волгоград: Изд-во ВолГУ, 2020. 95 с. ISBN 978-5-9669-1975-7. EDN SRVSDQ.

4. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. М.: РИОР: ИНФРА-М, 2019. 336 с. EDN URXUFR.

5. Баранова Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. 2009. № 1 (49). С. 15–26. EDN TMHRYF.

6. Полякова Т.А. Организационное и правовое обеспечение информационной безопасности: учеб. и практикум. М.: Юрайт, 2017. С. 54–56.

7. Васильев В.И., Вульфин А.М., Кудрявцева Р.Т. Анализ и управление рисками информационной безопасностью с использованием технологии когнитивного моделирования // Доклады Томского государственного университета систем управления и радиоэлектроники. 2017. Т. 20. № 4. С. 61–66. DOI: 10.21293/1818-0442-2017-20-4-61-66. EDN YTZQLP.

8. Паршенкова Ю.А., Максимова Е.А., Кунин Н.Т. Модель оценки кибербезопасности объектов критической информационной инфраструктуры // Информационная безопасность цифровой экономики: материалы XIX Науч.-практ. конф. (в рамках X Пленума регионального отделения Федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» по Сибирскому и Дальневосточному федеральным округам (СибРОУМО). Новосибирск: Сибирский гос. ун-т телеком. и информ., 2023. С. 69–75. EDN ECZVDV.

9. Papageorgiou E.I., Iakovidis D. Intuitionistic fuzzy cognitive maps // IEEE Trans. on Fuzzy Systems. DOI: 10.1109/ TFUZZ.2012.2214224.

10. Баранова С.Ю. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. 2015. № 1 (9). С. 73–79. EDN TNDTUP

11. Максимова Е.А. Инфраструктурный деструктивизм субъектов критической информационной инфраструктуры: монография. Волгоград: Волгоградский гос. ун-т, 2021. 181 с. ISBN 978-5-9669-2147-7. EDN ZZTOKE.

12. Knight Ch.J.K., Lloyd D.J.B., Penn A.S. Linear and Sigmoidal Fuzzy Cognitive Maps: An Analysis of Fixed Points // Applied Soft Computing. 2014. Vol. 15. P. 193–202. DOI: 10.1016/j.asoc.2013.10.030.

13. Stylios C.D., Georgopoulos V.C., Groumpos P.P. Intro- ducing the theory of fuzzy cognitive maps in distributed systems // Proc. of the Twelfth IEEE Intern. Symposium on Intelligent Control, 16–18 July 1997, Istanbul, Turkey, 1997. P. 55–60. DOI: 1109/ISIC.1997.626413.

14. Максименко В.Н., Ясюк Е.В. Сравнительный анализ методических подходов к оценке рисков информационной безопасности // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом: сб. материалов (тезисов) XXXIX Междунар. конф. РАЕН. Италия: ЗАО «НИРИТ», 2017. С. 15–16. EDN ZANIUD.

15. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 91–103. DOI: 10.31854/1813-324X-2020-6-4-91-103.

16. Yebiah-Bouteng E.O. Using fuzzy cognitive maps (FCMs) to evaluate the vulnerabilities with ICT assets disposal policies // International Journal of Electrical & Computer Sciences. 2012. Vol. 12. № 5. P. 20–31. URL: http://www.ijens.org/Vol_12_I_05/124705-8686-IJECS-IJENS.pdf.

References

1. Regional'nye sistemy. Inzhiniringovyj centr: Volgograd. URL: https://www.ec-rs.ru/blog/novosti/ataki-na-avtomatizirovannye-sistemy-upravleniya-tekhnologicheskimi-protsessam/ (data obrashcheniya: 21.06.2024).

2. Federal'naya sluzhba bezopasnosti Rossijskoj Federacii. URL: http://www.fsb.ru/fsb/press.htm (data obrashcheniya: 21.06.2024).

3. Maksimova E.A. Ocenka informacionnoj bezopasnosti sub"ekta kriticheskoj informacionnoj infrastruktury pri destruktivnyh vozdejstviyah. Volgograd: Izd-vo VolGU, 2020. 95 s. ISBN 978-5-9669-1975-7. EDN SRVSDQ.

4. Baranova E.K., Babash A.V. Informacionnaya bezopasnost' i zashchita informacii. M.: RIOR: INFRA-M, 2019. 336 s. EDN URXUFR.

5. Baranova E.K. Metodiki i programmnoe obespechenie dlya ocenki riskov v sfere informacionnoj bezopasnosti // Upravlenie riskom. 2009. № 1 (49). S. 15–26. EDN TMHRYF.

6. Polyakova T.A. Organizacionnoe i pravovoe obespechenie informacionnoj bezopasnosti: ucheb. i praktikum. M.: Yurajt, 2017. S. 54–56.

7. Vasil'ev V.I., Vul'fin A.M., Kudryavceva R.T. Analiz i upravlenie riskami informacionnoj bezopasnost'yu s ispol'zovaniem tekhnologii kognitivnogo modelirovaniya // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki. 2017. T. 20. № 4. S. 61–66. DOI: 10.21293/1818-0442-2017-20-4-61-66. EDN YTZQLP.

8. Parshenkova Yu.A., Maksimova E.A., Kunin N.T. Model' ocenki kiberbezopasnosti ob"ektov kriticheskoj informacionnoj infrastruktury // Informacionnaya bezopasnost' cifrovoj ekonomiki: materialy XIX Nauch.-prakt. konf. (v ramkah X Plenuma regional'nogo otdeleniya Federal'nogo uchebno-metodicheskogo ob"edineniya v sisteme vysshego obrazovaniya po ukrupnennoj gruppe special'nostej i napravlenij podgotovki 10.00.00 «Informacionnaya bezopasnost'» po Sibirskomu i Dal'nevostochnomu federal'nym okrugam (SibROUMO). Novosibirsk: Sibirskij gos. un-t telekom. i inform., 2023. S. 69–75. EDN ECZVDV.

9. Papageorgiou E.I., Iakovidis D. Intuitionistic fuzzy cognitive maps // IEEE Trans. on Fuzzy Systems. DOI: 10.1109/ TFUZZ.2012.2214224.

10. Baranova S.Yu. Metodiki analiza i ocenki riskov informacionnoj bezopasnosti // Obrazovatel'nye resursy i tekhnologii. 2015. № 1 (9). S. 73–79. EDN TNDTUP

11. Maksimova E.A. Infrastrukturnyj destruktivizm sub"ektov kriticheskoj informacionnoj infrastruktury: monografiya. Volgograd: Volgogradskij gos. un-t, 2021. 181 s. ISBN 978-5-9669-2147-7. EDN ZZTOKE.

12. Knight Ch.J.K., Lloyd D.J.B., Penn A.S. Linear and Sigmoidal Fuzzy Cognitive Maps: An Analysis of Fixed Points // Applied Soft Computing. 2014. Vol. 15. P. 193–202. DOI: 10.1016/j.asoc.2013.10.030.

13. Stylios C.D., Georgopoulos V.C., Groumpos P.P. Intro- ducing the theory of fuzzy cognitive maps in distributed systems // Proc. of the Twelfth IEEE Intern. Symposium on Intelligent Control, 16–18 July 1997, Istanbul, Turkey, 1997. P. 55–60. DOI: 10.1109/ISIC.1997.626413.

14. Maksimenko V.N., Yasyuk E.V. Sravnitel'nyj analiz metodicheskih podhodov k ocenke riskov informacionnoj bezopasnosti // Mobil'nyj biznes: perspektivy razvitiya i realizacii sistem radiosvyazi v Rossii i za rubezhom: sb. materialov (tezisov) XXXIX Mezhdunar. konf. RAEN. Italiya: ZAO «NIRIT», 2017. S. 15–16. EDN ZANIUD.

15. Maksimova E.A. Kognitivnoe modelirovanie destruktivnyh zloumyshlennyh vozdejstvij na ob"ektah kriticheskoj informacionnoj infrastruktury // Trudy uchebnyh zavedenij svyazi. 2020. T. 6. № 4. S. 91–103. DOI: 10.31854/1813-324X-2020-6-4-91-103.

16. Yebiah-Bouteng E.O. Using fuzzy cognitive maps (FCMs) to evaluate the vulnerabilities with ICT assets disposal policies // International Journal of Electrical & Computer Sciences. 2012. Vol. 12. № 5. P. 20–31. URL: http://www.ijens.org/Vol_12_I_05/124705-8686-IJECS-IJENS.pdf.

Информация о статье:
Статья поступила в редакцию: 13.08.2024; одобрена после рецензирования: 28.08.2024;
принята к публикации: 29.08.2024
Information about the article:
The article was submitted to the editorial office: 13.08.2024; approved after review: 28.08.2024;
accepted for publication: 29.08.2024

Сведения об авторах:
Паршенкова Юлия Анатольевна, ассистент кафедры «Информационно-аналитические системы кибербезопасности» Института кибербезопасности и цифровых технологий Российского технологического университета МИРЭА (119454, Москва, пр. Вернадского, д. 78), e-mail: parshenkova@mirea.ru, https://orcid.org/0009-0006-1965-6597, SPIN-код: 8186- 4893
Максимова Елена Александровна, профессор кафедры «Информационно-аналитические системы кибербезопасности» Института кибербезопасности и цифровых технологий Российского технологического университета МИРЭА (119454, Москва, пр. Вернадского, д. 78), доктор технических наук, доцент, e-mail: maksimova@mirea.ru, https://orcid.org/0000-0001-8788-4256
Матвеев Александр Владимирович, заведующий кафедрой прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат технических наук, доцент, e-mail: fcvega_10@mail.ru, https://orcid.org/0000-0002-0778-3218, SPIN-код: 5778-8832

Information about authors:
Parshenkova Yuliya A., assistant of the department of information and analytical systems of cybersecurity at the Institute of cybersecurity and digital technologies of the Russian technological university MIREA (119454, Moscow, Vernadsky ave., 78), e-mail: parshenkova@mirea.ru, https://orcid.org/0009-0006-1965-6597, SPIN: 8186-4893
Maksimova Elena A., professor of the department of information and analytical systems of cybersecurity at the Institute of cybersecurity and digital technologies of the Russian technological university MIREA (119454, Moscow, Vernadsky ave., 78), doctor of technical sciences, professor, e-mail: maksimova@mirea.ru, https://orcid.org/0000-0001-8788-4256
Matveev Alexander V., head of the department of applied mathematics and information technologies of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), candidate of technical sciences, associate professor, e-mail: fcvega_10@mail.ru, https://orcid.org/0000-0002-0778-3218, SPIN: 5778-8832