Научная статья
УДК 004.056; DOI: 10.61260/2218-13X-2024-2-91-104

ПРОАКТИВНОЕ МОДЕЛИРОВАНИЕ УТЕЧЕК ДАННЫХ ОГРАНИЧЕННОГО ДОСТУПА НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ (НА ПРИМЕРЕ ТРАНСПОРТНОЙ ОТРАСЛИ)

✉Утенкова Мария Александровна;
Максимова Елена Александровна.
МИРЭА – Российский технологический университет, Москва, Россия
✉utenkova@mirea.ru

Аннотация. Представлена комплексная методология прогнозирования утечек данных и оценки рисков вредоносного воздействия на объекты критической информационной инфраструктуры на примере транспортной отрасли. Проведен анализ статистических данных о количестве утечек данных ограниченного доступа в России за 2013–2022 гг. В рамках исследования сравнивается точность численных методов прогнозирования: линейная регрессия, сглаживание методами скользящей средней и экспоненциальное сглаживание. Был определен наиболее точный метод прогнозирования – линейная регрессия, который используется для прогнозирования утечек данных ограниченного доступа в транспортной отрасли на 2024–2028 гг. Кроме того, когнитивная модель позволяет оценить возможность утечек данных и их последствий с учетом таких факторов, как векторы атак, уязвимости системы, поведение пользователей, а также применяемых мер безопасности. Комбинированный подход при одновременном использовании численных методов и когнитивного моделирования обеспечивает целостное представление о рисках кибербезопасности, позволяя делать более точные прогнозы и принимать более обоснованные решения. Результаты исследования подчеркивают важность учета как технических, так и человеческих факторов при повышении кибербезопасности и предлагают рекомендации для будущих исследований по уточнению когнитивной модели с привлечением экспертов не только в технической, но и в экономической и юридической областях.

Ключевые слова: утечки данных, кибербезопасность, численное прогнозирование, когнитивное моделирование, критическая информационная инфраструктура, оценка рисков

Для цитирования: Утенкова М.А., Максимова Е.А. Проактивное моделирование утечек данных ограниченного доступа на объектах критической информационной инфраструктуры (на примере транспортной отрасли) // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 2. С. 91–104. DOI: 10.61260/2218-13X-2024-2-91-104.

Scientific article

PROACTIVE MODELING OF LIMITED ACCESS DATA LEAKS AT CRITICAL INFORMATION INFRASTRUCTURE FACILITIES (USING THE EXAMPLE OF THE TRANSPORT INDUSTRY)

✉Utenkova Maria A.;
Maximova Elena A.
MIREA – Russian university of technology, Moscow, Russia
✉utenkova@mirea.ru

Abstract. The article presents a comprehensive methodology for predicting data breaches and assessing the potential risks of harmful effects on critical information infrastructure, using

the example of the transport industry. Statistical data on the number of restricted access data leaks in Russia from 2013 to 2022 are analyzed. Within the study, several numerical forecasting methods are compared: linear regression, moving average smoothing, and exponential smoothing. Linear regression was found to be the most accurate method for predicting restricted access data leaks in the transport sector for 2024 to 2028. Additionally, a cognitive model is proposed that allows for assessing the likelihood of data breaches and their potential consequences, considering factors such as attack vectors, system vulnerabilities, user behavior, and implemented security measures. The combined approach, which combines numerical methods and cognitive modeling, provides a comprehensive view of cybersecurity risks. This allows for more accurate predictions and better-informed decisions. The study's results emphasize the importance of considering both technical and human aspects in improving cybersecurity, and offer recommendations for future research that could refine the cognitive model by involving experts from not only the technical field, but also the economic and legal domains.

Keywords: data leaks, cybersecurity, numerical forecasting, cognitive modeling, critical information infrastructure, risk assessment

For citation: Utenkova M.A., Maximova E.A. Proactive modeling of limited access data leaks at critical information infrastructure facilities (using the example of the transport industry) // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 2. P. 91–104. DOI: 10.61260/2218-13X-2024-2-91-104.

Введение

Транспортная отрасль, относящаяся к критической информационной инфраструктуре, в значительной степени зависит от информационных систем для обеспечения операций, связи и логистики [1]. Растущая цифровизация этих систем хотя и повышает их эффективность, но также подвергает их значительным рискам кибербезопасности. Утечки данных ограниченного доступа представляют собой серьезную угрозу конфиденциальности, целостности и доступности критически важной информации.

Многочисленные исследования выявили уязвимости в информационных системах транспортного сектора. Например, в исследованиях [2, 3] были рассмотрены риски, связанные с устаревшим программным обеспечением, недостаточными протоколами кибербезопасности, а также рисками, сопровождающими импортозамещение программного обеспечения. Кроме того, растущее использование устройств Интернета вещей (IoT) в транспортной инфраструктуре расширило возможности для атак, сделав системы более уязвимыми для кибератак [4].

Традиционные модели прогнозирования утечек данных в большей степени основаны на статистическом анализе и методах машинного обучения. В работе [5] авторы использовали логистическую регрессию и деревья решений для прогнозирования утечек данных, в то время как другие исследователи в работе [6] применили алгоритмы глубокого обучения для той же цели. Однако этим моделям часто не хватает возможности для учета неопределенности и сложности киберугроз, с которыми можно эффективно бороться с помощью нечеткой логики. Для проактивного моделирования активно используется методология когнитивного моделирования [7–12].

Целью данного исследования является разработка комплексной методологии прогнозирования утечек данных и оценки риска вредоносного воздействия на объекты критической информационной инфраструктуры на примере транспортной отрасли. Эта методология объединяет численные методы прогнозирования с нечетким когнитивным моделированием для учета неопределенностей и сложных взаимозависимостей между различными факторами риска, тем самым повышая точность и надежность прогнозов утечки данных и оценок рисков.

В задачи исследования входит:

– исследование статистических данных о количестве утечек данных ограниченного доступа в России за 10-летний период (2013–2022 гг.);

– анализ численных методов прогнозирования, включая линейную регрессию, методы скользящего среднего, методы взвешенного скользящего среднего и экспоненциального сглаживания;

– разработка математической модели для прогнозирования утечек данных ограниченного доступа с использованием метода численного прогнозирования, показавшего наибольшую точность в прогнозировании утечек данных;

– разработка когнитивной модели для оценки вероятности и потенциальных последствий утечек данных;

– моделирование различных сценариев развития событий информационной безопасности с использованием когнитивной модели.

Методы исследования

Прогнозирование утечек данных объединяет численное прогнозирование и методы нечеткого моделирования для учета неопределенностей во входных переменных. Для повышения точности прогнозирования используются несколько численных методов, включая линейную регрессию, методы скользящего среднего, методы взвешенного скользящего среднего и экспоненциального сглаживания. Эти методы выбраны из-за их доказанной эффективности в прогнозировании и обработке данных временных рядов:

1. Линейная регрессия. Распространенный статистический метод, используемый для моделирования взаимосвязи между зависимой переменной и одной или несколькими независимыми переменными. Линейная регрессия эффективна при выявлении тенденций и составлении прогнозов на основе исторических данных [13–15].

2. Методы скользящей средней. Используются для сглаживания краткосрочных колебаний и выявления долгосрочных тенденций в данных. Простые скользящие средние вычисляют среднее значение точек данных в пределах заданного интервала, что делает их пригодными для данных без четкого тренда или сезонной закономерности [16].

3. Экспоненциальное сглаживание. Метод прогнозирования, который применяет уменьшающиеся веса к прошлым данным, уделяя больше внимания недавним наблюдениям. Экспоненциальное сглаживание особенно эффективно для данных с трендами или сезонными колебаниями [17, 18].

Когнитивное моделирование применяется для управления сложными системами, характеризующимися неопределенностью и неточностями. Когнитивная модель позволяет представлять причинно-следственные связи между факторами в системе с использованием нечеткой логики, что делает его мощным инструментом для анализа и прогнозирования поведения в динамичных и неопределенных средах, таких как кибербезопасность [9–11, 19–22].

Исследование включает три основных этапа:

1. На основе статистики количества утечек данных ограниченного доступа в России за 10 лет с 2013 по 2022 г. от компании InfoWatch [23] строится линейная регрессия со сглаживанием и без, где в качестве зависимого параметра выступает количество утечек (рис. 1). По полученным математическим моделям «прогнозируется» количество утечек для 2023 г., после чего сравнивается с фактическим значением за этот год.

2. Выбирается метод прогнозирования количества утечек данных, показавший наиболее точное совпадение с фактическими данными. С применением данного метода строится математическая модель на основе статистики количества утечек данных ограниченного доступа в транспортной отрасли за 2019–2023 гг. от компании InfoWatch (рис. 2) [24–28]. В результате вычисляется прогнозируемое количество утечек данных для 2024–2028 гг.

3. Построение когнитивной модели для оценки вероятности утечки данных ограниченного доступа и потерь в случае наступления утечки данных. Проведение ряда экспериментов для определения того, как входные данные влияют на результирующие концепты.

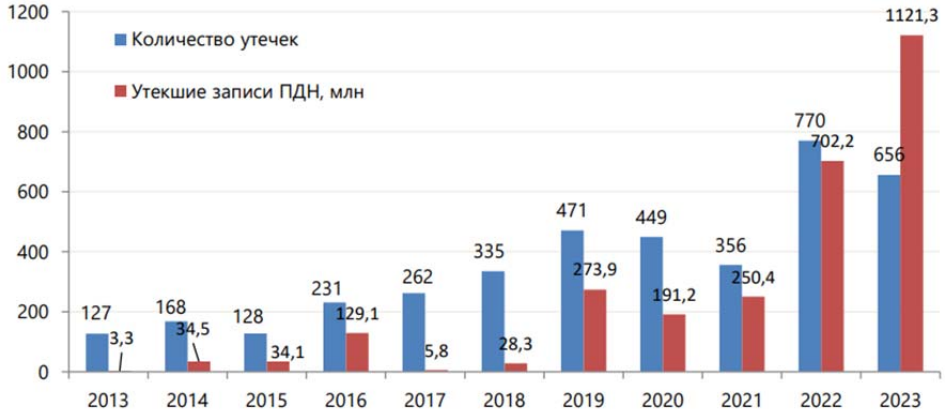

Рис. 1. **Количество утечек информации в России, 2013–2023 гг.**

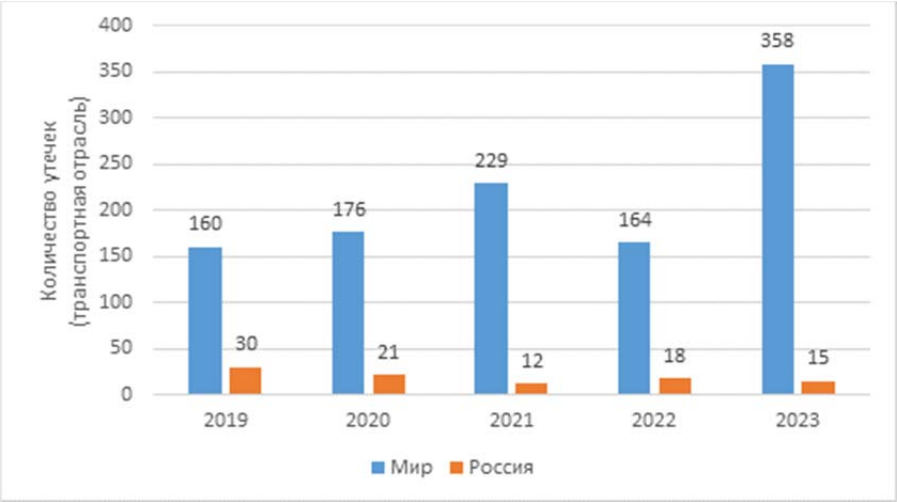

Рис. 2. **Количество утечек в транспортной отрасли: Россия – Мир, 2019–2023 гг.**

На первом этапе исследования рассматриваются четыре метода численного прогнозирования:

1. Линейная регрессия на основе статистики за 2013–2022 гг.:

$$y = 57{,}5818x - 115841{,}6182,$$

при x = 2023, y = 646,3632.

2. Результат сглаживания статистических данных о количестве утечек за 2013–2022 гг. с использованием метода односторонней скользящей средней представлен в табл. 1 (период усреднения равен 3).

Таблица 1

Количество утечек данных ограниченного доступа за 2013–2022 гг. после сглаживания методом односторонней скользящей средней

Год	Количество утечек	Год	Количество утечек
2013	127	2018	276
2014	140,67	2019	356
2015	141	2020	418,33
2016	175,67	2021	425,33
2017	207	2022	525

Линейная регрессия на основе сглаженных данных:

$$y = 45{,}8864x - 92296{,}6609,$$

при x = 2023, y = 531,527.

3. Результат сглаживания статистических данных за 2013–2022 гг. с использованием метода двусторонней скользящей средней представлен в табл. 2 (период усреднения равен 3).

Таблица 2

Количество утечек данных ограниченного доступа за 2013–2022 гг. после сглаживания методом двусторонней скользящей средней

Год	Количество утечек	Год	Количество утечек
2013	140,67	2018	356
2014	141	2019	418,33
2015	175,67	2020	425,33
2016	207	2021	525
2017	276	2022	632

Линейная регрессия на основе сглаженных данных:

$$y = 54{,}9834x - 110599{,}2973,$$

при x = 2023, y = 632,1209.

4. Результат сглаживания статистических данных за 2013–2022 гг. с использованием метода экспоненциального сглаживания представлен в табл. 3.

Таблица 3

Количество утечек данных ограниченного доступа за 2013–2022 гг. после применения метода экспоненциального сглаживания

Год	Количество утечек	Год	Количество утечек
2013	127	2018	307,75
2014	155,69	2019	422,02
2015	136,3	2020	440,9
2016	202,59	2021	381,47
2017	244,17	2022	653,4

Линейная регрессия на основе сглаженных данных:

$$y = 51{,}8965x - 104394{,}1515,$$

при x = 2023, y = 592,468.

В результате сравнения спрогнозированных значений для 2023 г. с фактическим количеством утечек данных ограниченного доступа в 2023 г. наиболее точным для прогнозирования показал себя метод линейной регрессии без сглаживания.

На втором этапе исследования построена математическая модель методом линейной регрессии на основе статистики количества утечек данных ограниченного доступа в транспортной отрасли за 2019–2023 гг.:

$$y = 38{,}4x - 77389.$$

Полученная математическая модель позволяет вычислить прогнозируемое количество утечек данных ограниченного доступа в транспортной отрасли для ближайших нескольких лет. Результат прогнозирования представлен в табл. 4.

Таблица 4

Прогнозируемое количество утечек данных ограниченного доступа в транспортной отрасли на 2024–2028 гг.

Год	Количество утечек (факт.)	Год	Количество утечек (прогноз.)
2019	160	2024	332,6
2020	176	2025	371
2021	229	2026	409,4
2022	164	2027	447,8
2023	358	2028	486,2

На третьем этапе исследования разработана когнитивная модель для оценки возможности утечек данных из защищаемого контура некоторой организации и потерь, которые понесет организация в случае утечки данных (рис. 2).

Все элементы модели (концепты) разделены на три группы:

1. Входные концепты: «векторы атаки», «уязвимости системы», «поведение пользователя», «меры безопасности», «стоимость активов», «средства для обнаружения и реагирования на инцидент».
2. Промежуточные концепты: «уровень угрозы», «уровень уязвимости».
3. Выходные концепты: «потери в связи с утечкой», «оценка возможности утечки».

Принято, что связи между концептами могут быть с коэффициентом «1» (обозначается символом «+»), что означает прямое влияние родительского концепта на дочерний, или с коэффициентом «-1» (обозначается символом «-»), что означает обратное влияние (рис. 3). Каждый входной концепт может принимать значение от «-1» до «1» (рис. 4).

В ходе моделирования с использованием полученной когнитивной модели рассматривались следующие случаи:

1. Все входные концепты принимают значение «1» (рис. 5).
2. Все входные концепты принимают значение «-1» (рис. 6).
3. Входные концепты: «векторы атаки», «уязвимости системы», «поведение пользователя», «меры безопасности», «стоимость активов» принимают значение «1», а «меры безопасности» и «средства для обнаружения и реагирования на инцидент» – «-1» (рис. 7).
4. Входные концепты: «векторы атаки», «уязвимости системы», «поведение пользователя», «меры безопасности», «стоимость активов» принимают значение «-1», а «меры безопасности» и «средства для обнаружения и реагирования на инцидент» – «1» (рис. 8).

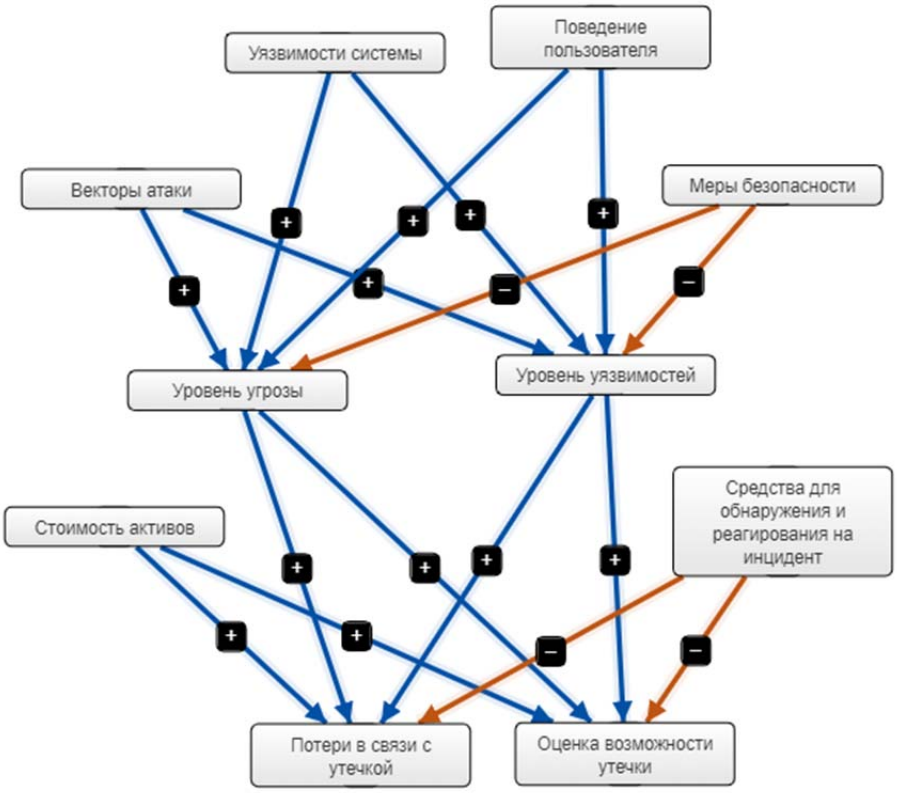

Рис. 3. **Когнитивная модель оценки возможности утечек и потерь в связи с утечкой**

Рис. 4. **Шкала значений концептов когнитивной модели**

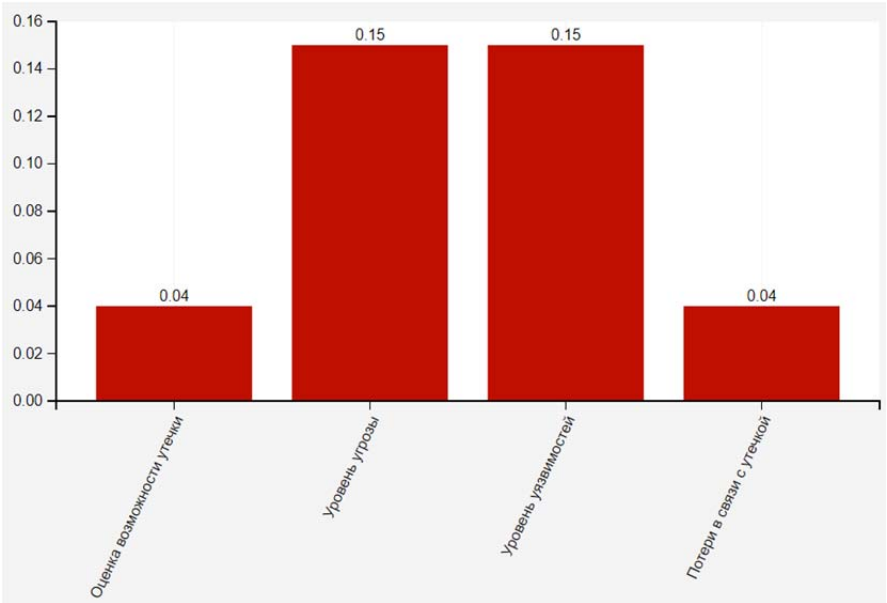

Рис. 5. **Результат моделирования случая:**
все входные концепты принимают значение «1»

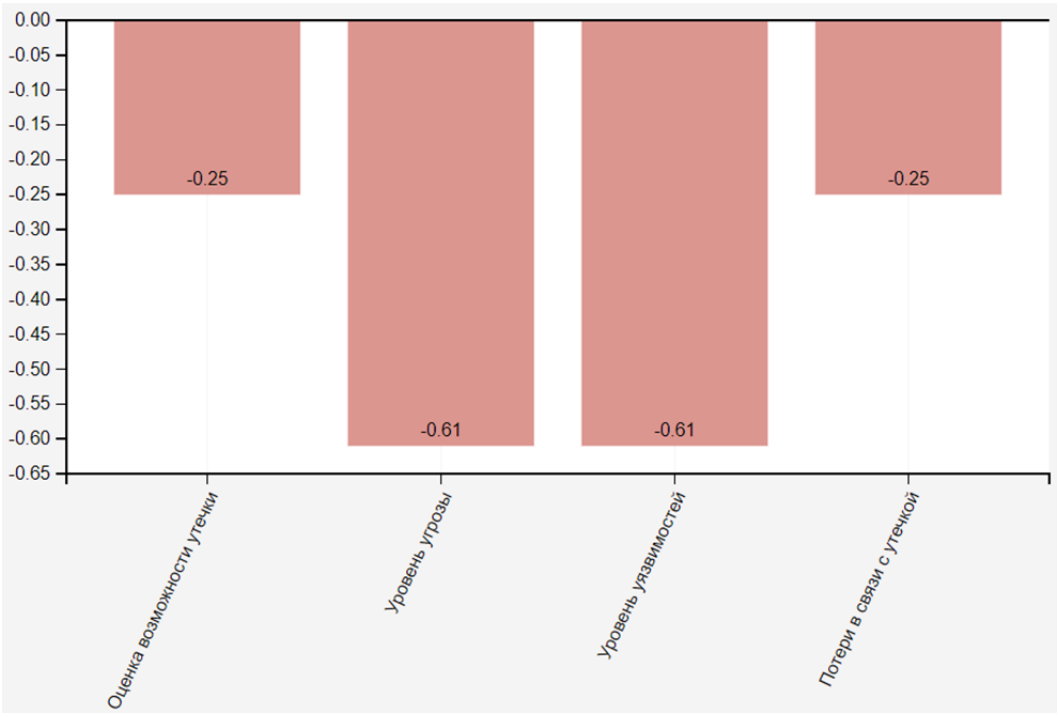

Рис. 6. **Результат моделирования случая:**
все входные концепты принимают значение «-1»

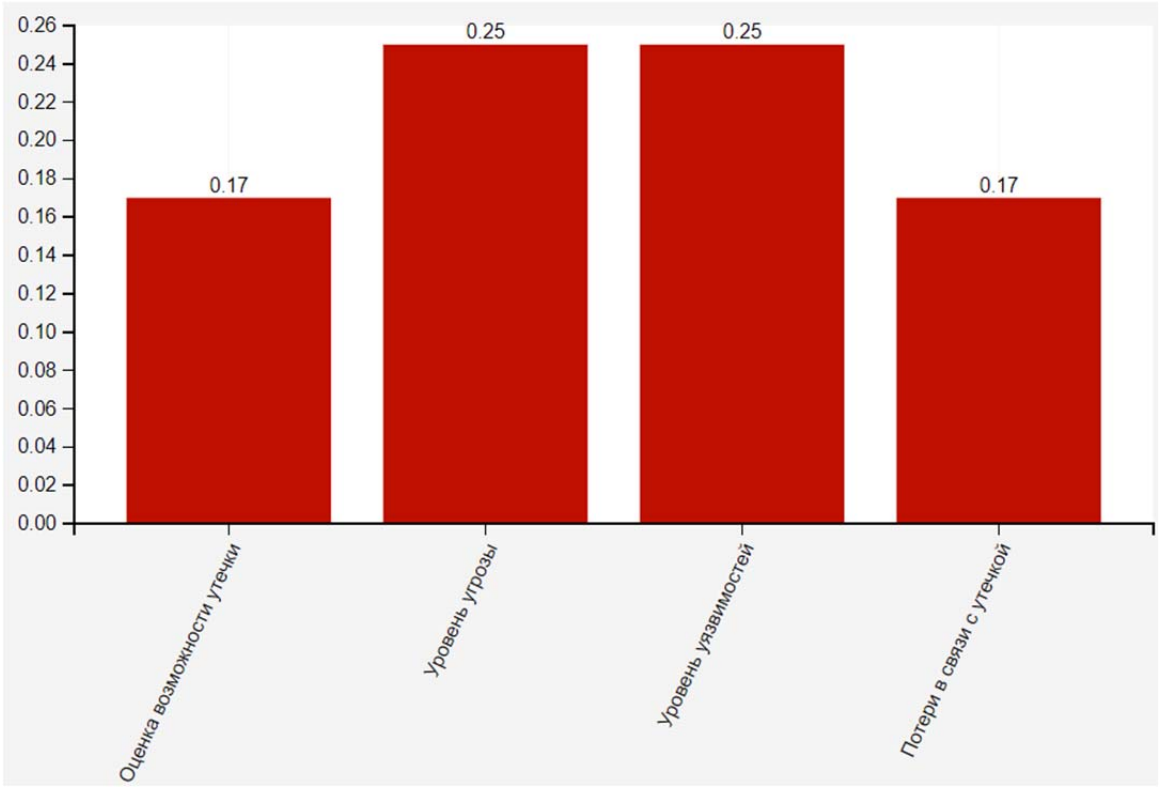

Рис. 7. **Результат моделирования случая:**
входные концепты: «векторы атаки», «уязвимости системы»,
«поведение пользователя», «меры безопасности», «стоимость активов»
принимают значение «1», а «меры безопасности»
и «средства для обнаружения и реагирования на инцидент» – «-1»

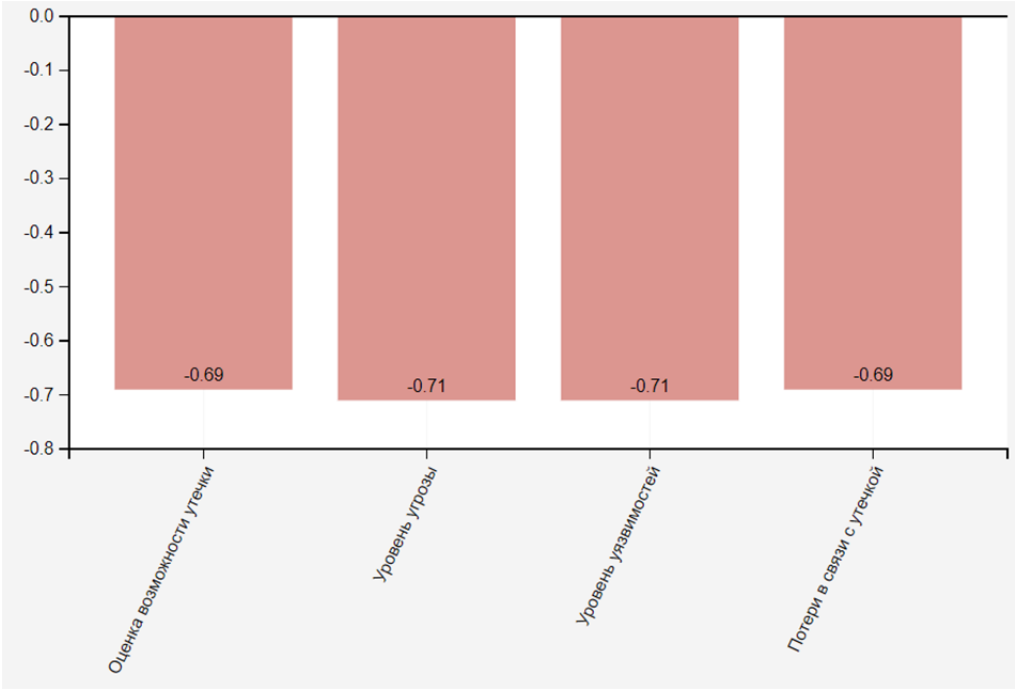

Рис. 8. **Результат моделирования случая:
входные концепты: «векторы атаки», «уязвимости системы»,
«поведение пользователя», «меры безопасности»,
«стоимость активов» принимают значение «-1»,
а «меры безопасности» и «средства для обнаружения и реагирования на инцидент» – «1»**

Результаты исследования и их обсуждение

При изучении статистических данных о количестве утечек данных ограниченного доступа прослеживается увеличение количества утечек данных ограниченного доступа и утекших записей персональных данных по всем отраслям за 11 лет, начиная с 2013 г. Заметен значительный рост, особенно в 2022–2023 гг. Это во многом связано как с повсеместным внедрением сервисов для удаленной работы на фоне карантина в 2020–2021 гг., так и с обострившейся геополитической ситуацией в мире. По первой причине были в срочном порядке внедрены сервисы, которые из-за срочности и внезапности задач не отвечали требованиям обеспечения безопасности, то есть степень защищенности системы значительно снизилась. Дома сотрудники также не всегда должным образом защищали свои рабочие устройства от членов семьи, которые по неосторожности или намеренно могли поспособствовать утечке данных. А обострение геополитической обстановки спровоцировало возросший к интерес критической информационной инфраструктуре со стороны зарубежных нарушителей.

Аналогичная ситуация прослеживается и в случае с утечками данных в транспортной отрасли с 2019 по 2023 г. Данная отрасль имеет стратегически важное значение для России как в экономическом, так и в военном плане. В связи с этим число утечек данных в данной отрасли растет. В рамках исследования спрогнозирована дальнейшая динамика роста данного показателя: через пять лет планируется увеличение почти в полтора раза. Стоит отметить, что при прогнозировании не были учтены случайные факторы, которые в значительной мере могли бы в дальнейшем повлиять на интерес нарушителей информационной безопасности к данным ограниченного доступа.

Моделирование при помощи полученной когнитивной модели показало, что для снижения риска утечек данных ограниченного доступа компании необходимо улучшать защиту данных в инфраструктуре организации. Для этого необходимо закрывать известные уязвимости в используемом программном обеспечении, обучать сотрудников и применять дополнительные меры защиты данных.

Заключение

Представленные в исследовании методы позволяют выполнить моделирование утечек данных с разной степенью погрешности и могут использоваться как на уровне отдельной организации, так и для всей отрасли в целом. Данные методы позволяют решать разные задачи при помощи моделирования: численные методы выполняют прогнозные задачи исходя из имеющейся статистики, а с помощью когнитивной карты можно оценить возможность свершения некоторого события информационной безопасности, а также определить элементы инфраструктуры, которые нуждаются в улучшении мер по обеспечению безопасности в первую очередь. Для получения наилучшего результата при защите от утечек данных ограниченного доступа рекомендуется использовать представленные методы моделирования вместе.

Предложенная когнитивная модель требует доработки. В данном вопросе необходимо будет опираться на экспертные мнения специалистов не только в технической, но и экономической и юридической отраслях, что позволит рассматривать процесс обеспечения кибербезопасности организации не изолированно, а как часть бизнес-процессов.

Список источников

1. О безопасности критической информационной инфраструктуры Российской Федерации: Федер. закон Рос. Федерации от 26 июля 2017 г. № 187-ФЗ (последняя ред.). Доступ из инф.-правового портала «Гарант».

2. Сафонова М.Ф., Ципляева С.А. Кибербезопасность: проблемы и решения // ЕГИ. 2019. № 24 (2). С. 63–68.

3. Торосян Е.К., Торопчинова А.Д. Вопросы управления рисками IT-проектов при переходе на новое программное обеспечение в современных условиях // Петербургский экономический журнал. 2018. № 3. С. 105–109.

4. Панин Д.Н., Бобков Е.О., Балашова Е.А. Анализ кибератак на критическую информационную инфраструктуру с IoT технологиями // Автономия личности. 2020. № 2 (22). С. 55–64.

5. Базылев В.В., Карнахин В.А. Сравнение возможностей логистической регрессии и искусственных нейронных сетей в прогнозировании результатов исследования на малой выборке // Health, Food & Biotechnology. 2019. № 3. С. 11–20.

6. Староверов Б.А., Хамитов Р.Н. Реализация глубокого обучения для прогнозирования при помощи ансамбля нейронных сетей // Известия ТулГУ. Технические науки. 2023. № 4. 185–189.

7. Castro J.L., Delgado M. Fuzzy systems with defuzzification are universal approximators // IEEE Transactions on Systems, Man and Cybernetics. Part B (Cybernetics). 1996. Vol. 26. Iss. 1. P. 149–152.

8. Fuzzy cognitive mapping as a tool to define management objectives for complex ecosystems / B.F. Hobbs [et al.] // Ecol. Appl. 2002. № 12. P. 1548–1565.

9. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 91–103.

10. Садовникова Н.П., Ермощенко К. Общие вопросы применения методологии имитационного моделирования для оценки эколого-экономической эффективности проектов градостроительной деятельности // Известия Волгоградского государственного технического университета. 2011. № 9 (82). С. 94–97.

11. Садовникова Н.П., Жидкова Н.П. Выбор стратегий территориального развития на основе когнитивного анализа и сценарного моделирования // Интернет-вестник ВолгГАСУ. 2012. № 7 (21). С. 4.

12. Максимова Е.А., Садовникова Н.А., Парыгин Д.С. Прогнозирование деструктивных воздействий на объектах критической информационной инфраструктуры // Информационные технологии и технологии коммуникаций. Современные достижения:

материалы IV Междунар. науч. конф., посвящ. 90-летию со дня основания Астраханского гос. техн. ун-та. Астрахань: Астраханский гос. техн. ун-т, 2020. С. 25.

13. Гржибовский А.М. Однофакторный линейный регрессионный анализ // Экология человека. 2008. № 10. С. 55–64.

14. Утенкова М.А. Численное прогнозирование утечек данных ограниченного доступа // Актуальные проблемы прикладной математики, информатики и механики: сб. трудов Междунар. науч. конф. Воронеж: ООО «Вэлборн»; Изд-во «Научно-исследовательские публикации», 2024. С. 721–725. EDN CZBTNX.

15. Максимова Е.А., Утенкова М.А. Прогнозирование развития событий в ходе информационного противоборства // Студенческая наука для развития информационного общества: материалы XV Всерос. науч.-техн. конф. с приглашением зарубежных ученых. Ставрополь: Северо-Кавказский федер. ун-т, 2024. С. 209–218. EDN NUSUUD.

16. Marimuthu K., Gopinath M. Production of Sugarcane Forecasting using ARIMAX Model // Scopus. International Journal of Innovative Technology and Exploring Engineering. 2019. Vol. 8. Iss. 12-S.

17. Gardner Everette. Exponential smoothing: the state of the art – Part II // International Journal of Forecasting. 2006. № 22. P. 637–666.

18. Hwang S.H., Chen H.T., Chang C.T. An exponentially weighted moving average method for identification and monitoring of stochastic systems // Industrial and Engineering Chemistry Research. № 47 (21). P. 8239–8249. DOI: 10.1021/ie0707218.

19. Утенкова М.А., Максимова Е.А. Нечеткое моделирование сценарного развития гибридной войны // Цифровая трансформация науки и образования: сб. науч. трудов IV Всерос. науч.-практ. конф. с междунар. участием. Нальчик: Кабардино-Балкарский гос. ун-т им. Х.М. Бербекова, 2023. С. 355–360.

20. Vatankhah G., Tarafdar H., Ghassem Z. Fermat-curve based fuzzy inference system for the fuzzy logic controller performance optimization in load frequency control application // Fuzzy Optim Decis Making. 2023. № 22. P. 555–586. DOI: 1007/s10700-022-09402-2.

21. An agile FCM for real-time modeling of dynamic and reallife systems, evolving systems / O. Motlagh [et al.] // Special issue on temporal aspects in fuzzy cognitive maps. 2013. P. 137–145.

22. Obiedat M., Samarasinghe S. Fuzzy representation and aggregation of fuzzy cognitive maps // 20th International Congress on Modelling and Simulation. Adelaide, Australia, 2013. P. 690–694.

23. Утечки информации в мире, 2022–2023 годы: аналитический отчет. URL: https://www.infowatch.ru/sites/default/files/analytics/files/issledovaniye-utechek-informatsii-v-mire-za-2022-2023-gody.pdf (дата обращения: 03.05.2024).

24. Аналитические отчеты. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_РоссияУтечки_за2019.pdf (дата обращения: 03.05.2024).

25. Исследование утечек информации ограниченного доступа в 2019 году: аналитический отчет. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_МирУтечки_за2019.pdf (дата обращения: 03.05.2024).

26. Россия: утечки информации ограниченного доступа, 2020 год: аналитический отчет. URL: https://www.infowatch.ru/sites/default/files/analytics/files/c_IW_Россия_2020_утечки_v%201%207%201пп%20%282%29.pdf (дата обращения: 03.05.2024).

27. Исследование утечек информации ограниченного доступа в 2020 году: аналитический отчет. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения: 03.05.2024).

28. Россия: утечки информации ограниченного доступа, 2022–2023 годы: аналитический отчет. URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-2023.pdf (дата обращения: 03.05.2024).

References

1. O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii: Feder. zakon Ros. Federacii ot 26 iyulya 2017 g. № 187-FZ (poslednyaya red.). Dostup iz inf.-pravovogo portala «Garant».

2. Safonova M.F., Ciplyaeva S.A. Kiberbezopasnost': problemy i resheniya // EGI. 2019. № 24 (2). S. 63–68.

3. Torosyan E.K., Toropchinova A.D. Voprosy upravleniya riskami IT-proektov pri perekhode na novoe programmnoe obespechenie v sovremennyh usloviyah // Peterburgskij ekonomicheskij zhurnal. 2018. № 3. S. 105–109.

4. Panin D.N., Bobkov E.O., Balashova E.A. Analiz kiberatak na kriticheskuyu informacionnuyu infrastrukturu s IoT tekhnologiyami // Avtonomiya lichnosti. 2020. № 2 (22). S. 55–64.

5. Bazylev V.V., Karnahin V.A. Sravnenie vozmozhnostej logisticheskoj regressii i iskusstvennyh nejronnyh setej v prognozirovanii rezul'tatov issledovaniya na maloj vyborke // Health, Food & Biotechnology. 2019. № 3. S. 11–20.

6. Staroverov B.A., Hamitov R.N. Realizaciya glubokogo obucheniya dlya prognozirovaniya pri pomoshchi ansamblya nejronnyh setej // Izvestiya TulGU. Tekhnicheskie nauki. 2023. № 4. 185–189.

7. Castro J.L., Delgado M. Fuzzy systems with defuzzification are universal approximators // IEEE Transactions on Systems, Man and Cybernetics. Part B (Cybernetics). 1996. Vol. 26. Iss. 1. P. 149–152.

8. Fuzzy cognitive mapping as a tool to define management objectives for complex ecosystems / B.F. Hobbs [et al.] // Ecol. Appl. 2002. № 12. P. 1548–1565.

9. 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.

10. Sadovnikova N.P., Ermoshchenko K. Obshchie voprosy primeneniya metodologii imitacionnogo modelirovaniya dlya ocenki ekologo-ekonomicheskoj effektivnosti proektov gradostroitel'noj deyatel'nosti // Izvestiya Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. 2011. № 9 (82). S. 94–97.

11. Sadovnikova N.P., Zhidkova N.P. Vybor strategij territorial'nogo razvitiya na osnove kognitivnogo analiza i scenarnogo modelirovaniya // Internet-vestnik VolgGASU. 2012. № 7 (21). S. 4.

12. Maksimova E.A., Sadovnikova N.A., Parygin D.S. Prognozirovanie destruktivnyh vozdejstvij na ob"ektah kriticheskoj informacionnoj infrastruktury // Informacionnye tekhnologii i tekhnologii kommunikacij. Sovremennye dostizheniya: materialy IV Mezhdunar. nauch. konf., posvyashch. 90-letiyu so dnya osnovaniya Astrahanskogo gos. tekhn. un-ta. Astrahan': Astrahanskij gos. tekhn. un-t, 2020. S. 25.

13. Grzhibovskij A.M. Odnofaktornyj linejnyj regressionnyj analiz // Ekologiya cheloveka. 2008. № 10. S. 55–64.

14. Utenkova M.A. Chislennoe prognozirovanie utechek dannyh ogranichennogo dostupa // Aktual'nye problemy prikladnoj matematiki, informatiki i mekhaniki: sb. trudov Mezhdunar. nauch. konf. Voronezh: OOO «Velborn»; Izd-vo «Nauchno-issledovatel'skie publikacii», 2024. S. 721–725. EDN CZBTNX.

15. Maksimova E.A., Utenkova M.A. Prognozirovanie razvitiya sobytij v hode informacionnogo protivoborstva // Studencheskaya nauka dlya razvitiya informacionnogo obshchestva: materialy XV Vseros. nauch.-tekhn. konf. s priglasheniem zarubezhnyh uchenyh. Stavropol': Severo-Kavkazskij feder. un-t, 2024. S. 209–218. EDN NUSUUD.

16. Marimuthu K., Gopinath M. Production of Sugarcane Forecasting using ARIMAX Model // Scopus. International Journal of Innovative Technology and Exploring Engineering. 2019. Vol. 8. Iss. 12-S.

17. Gardner Everette. Exponential smoothing: the state of the art – Part II // International Journal of Forecasting. 2006. № 22. P. 637–666.

18. Hwang S.H., Chen H.T., Chang C.T. An exponentially weighted moving average method for identification and monitoring of stochastic systems // Industrial and Engineering Chemistry Research. № 47 (21). P. 8239–8249. DOI: 10.1021/ie0707218.

19. Utenkova M.A., Maksimova E.A. Nechetkoe modelirovanie scenarnogo razvitiya gibridnoj vojny // Cifrovaya transformaciya nauki i obrazovaniya: sb. nauch. trudov IV Vseros. nauch.-prakt. konf. s mezhdunar. uchastiem. Nal'chik: Kabardino-Balkarskij gos. un-t im. H.M. Berbekova, 2023. S. 355–360.

20. Vatankhah G., Tarafdar H., Ghassem Z. Fermat-curve based fuzzy inference system for the fuzzy logic controller performance optimization in load frequency control application // Fuzzy Optim Decis Making. 2023. № 22. P. 555–586. DOI: 1007/s10700-022-09402-2.

21. An agile FCM for real-time modeling of dynamic and reallife systems, evolving systems / O. Motlagh [et al.] // Special issue on temporal aspects in fuzzy cognitive maps. 2013. P. 137–145.

22. Obiedat M., Samarasinghe S. Fuzzy representation and aggregation of fuzzy cognitive maps // 20th International Congress on Modelling and Simulation. Adelaide, Australia, 2013. P. 690–694.

23. Utechki informacii v mire, 2022–2023 gody: analiticheskij otchet. URL: https://www.infowatch.ru/sites/default/files/analytics/files/issledovaniye-utechek-informatsii-v-mire-za-2022-2023-gody.pdf (data obrashcheniya: 03.05.2024).

24. Analiticheskie otchety. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_RossiyaUtechki_za2019.pdf (data obrashcheniya: 03.05.2024).

25. Issledovanie utechek informacii ogranichennogo dostupa v 2019 godu: analiticheskij otchet. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_MirUtechki_za2019.pdf (data obrashcheniya: 03.05.2024).

26. Rossiya: utechki informacii ogranichennogo dostupa, 2020 god: analiticheskij otchet. URL: https://www.infowatch.ru/sites/default/files/analytics/files/c_IW_Rossiya_2020_utechki_v%201%207%201pp%20%282%29.pdf (data obrashcheniya: 03.05.2024).

27. Issledovanie utechek informacii ogranichennogo dostupa v 2020 godu: analiticheskij otchet. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Mir_Utechki_2020_v.1.17.pdf (data obrashcheniya: 03.05.2024).

28. Rossiya: utechki informacii ogranichennogo dostupa, 2022–2023 gody: analiticheskij otchet. URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-2023.pdf (data obrashcheniya: 03.05.2024).

Информация о статье:
Статья поступила в редакцию: 10.05.2024; одобрена после рецензирования: 24.06.2024;
принята к публикации: 25.06.2024

The information about article:
The article was submitted to the editorial office: 10.05.2024; approved after review: 24.06.2024;
accepted for publication: 25.06.2024

Информация об авторах:
Утенкова Мария Александровна, обучающийся кафедры КБ-2 «Информационно-аналитические системы кибербезопасности» МИРЭА – Российского технологического университета (119454, Москва, пр. Вернадского, д. 78), e-mail: utenkova@mirea.ru, https://orcid.org/0009-0003-9857-3754, SPIN-код: 3629-2516
Максимова Елена Александровна, исполняющий обязанности заведующего кафедрой КБ-9 «Предметно-ориентированные информационные системы» МИРЭА – Российского технологического университета; профессор кафедры КБ-2 «Информационно-аналитические системы кибербезопасности» МИРЭА – Российского технологического университета (119454, Москва, пр. Вернадского, д. 78), доктор технических наук, e-mail: maksimova@mirea.ru, https://orcid.org/0000-0001-8788-4256, SPIN-код: 6876-5558

Information about the authors:
Utenkova Maria A., student department KB-2 «Information and analytical systems of cybersecurity» of MIREA – Russian university of technology (119454, Moscow, Vernadsky ave, 78), e-mail: utenkova@mirea.ru, https://orcid.org/0009-0003-9857-3754, SPIN: 3629-2516
Maksimova Elena A., acting head of the department KB-9 «Subject-oriented information systems» of MIREA – Russian university of technology; professor of the department KB-2 «Information and analytical systems of cybersecurity» MIREA – Russian university of technology (119454, Moscow, Vernadsky ave., 78), doctor of technical sciences, e-mail: maksimova@mirea.ru, https://orcid.org/0000-0001-8788-4256, SPIN: 6876-5558