DOI: 10.25559/SITITO.020.202401.70-81
УДК 004.81

Оригинальная статья

Применение технологий машинного обучения для управления многофакторными угрозами в интегрированной модели когнитивного центра безопасности на предприятии оборонно-промышленного комплекса

П. А. Панилов*, Т. Ю. Цибизова
ФГБОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)», г. Москва, Российская Федерация
Адрес: 105005, Российская Федерация, г. Москва, ул. 2-я Бауманская, д. 5, к. 1
* panilovp.a@bmstu.ru

Аннотация
Представленная модель когнитивного центра безопасности, опирающаяся на технологии машинного обучения, представляет собой важный шаг в эффективном управлении многофакторными угрозами на предприятиях оборонно-промышленного комплекса (ОПК). В данной статье детально рассматриваются ключевые элементы этой модели, включая анализ данных, выявление аномалий, реакцию на угрозы, классификацию и оптимизацию, а также систему оповещения. Особое внимание уделяется способности модели объединять данные из различных источников в режиме реального времени, что обеспечивает оперативное реагирование на разнообразные угрозы и создает полное представление о безопасности предприятия. Модель успешно демонстрирует применение алгоритмов машинного обучения, эффективно обрабатывая аномалии и реагируя на угрозы, предоставляя оперативные решения для управления безопасностью в реальном времени. Кроме того, в статье подчеркивается значимость динамичной адаптации алгоритмов машинного обучения к новым угрозам, придавая системе устойчивость в постоянно меняющейся среде безопасности. Эффективное управление реакцией на угрозы обеспечивается автоматизированными протоколами безопасности, ускоряя процесс принятия решений и существенно уменьшая потенциальные риски для предприятия. Важной составляющей модели является роль системы оповещения, которая играет ключевую роль в оперативной связи с персоналом безопасности и ответственными структурами при обнаружении угрозы. Это обеспечивает быстрое и целенаправленное воздействие, направленное на нейтрализацию угрозы или минимизацию ее возможных последствий. Такой современный и эффективный подход к управлению безопасностью обеспечивает всесторонний и интегрированный подход к обеспечению безопасности на предприятии оборонно-промышленного комплекса, предоставляя защиту в реальном времени.

Ключевые слова: интегрированная модель, когнитивный центр безопасности, машинное обучение, анализ данных, выявление аномалий, реакция на угрозы, оперативное реагирование, многофакторные угрозы

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Панилов П. А., Цибизова Т. Ю. Применение технологий машинного обучения для управления многофакторными угрозами в интегрированной модели когнитивного центра безопасности на предприятии оборонно-промышленного комплекса // Современные информационные технологии и ИТ-образование. 2024. Т. 20, № 1. С. 70-81. https://doi.org/10.25559/SITITO.020.202401.70-81

Original article

Application of Machine Learning Technologies for Managing Multifactor Threats in an Integrated Model of Cognitive Security Center at Defense Industry Enterprise

P. A. Panilov*, T. Yu. Tsybizova
Bauman Moscow State Technical University, Moscow, Russian Federation
Address: 5, 2nd Baumanskaya St., building 2, Moscow 105005, Russian Federation
* panilovp.a@bmstu.ru

Abstract

The presented innovative model of the cognitive security center, based on machine learning technologies, represents a significant advancement in effectively managing multifactor threats in defense-industrial complex enterprises. This article provides a detailed examination of key elements of this model, including data analysis, anomaly detection, threat response, classification and optimization, as well as the notification system. Particular attention is given to the model's ability to integrate data from various sources in real-time, enabling swift responses to diverse threats and providing a comprehensive overview of the enterprise's security. The model effectively demonstrates the application of machine learning algorithms, efficiently processing anomalies and responding to threats, offering real-time operational security management solutions. Additionally, the article underscores the importance of the dynamic adaptation of machine learning algorithms to new threats, imparting resilience to the system in a constantly changing security environment. Efficient threat response management is ensured through automated security protocols, expediting decision-making processes and significantly reducing potential risks for the enterprise. A crucial component of the model is the role of the notification system, playing a key role in operational communication with security personnel and responsible structures upon threat detection. This facilitates swift and targeted actions, directed towards neutralizing the threat or minimizing its potential consequences. Such a modern and effective approach to security management provides a comprehensive and integrated strategy for ensuring security in defense-industrial complex enterprises, offering real-time protection.

Keywords: integrated model, cognitive security center, machine learning, data analysis, anomaly detection, threat response, real-time response, multifactor threats

Conflict of interests: The authors declare no conflict of interest.

For citation: Panilov P.A., Tsybizova T.Yu. Application of Machine Learning Technologies for Managing Multifactor Threats in an Integrated Model of Cognitive Security Center at Defense Industry Enterprise. *Modern Information Technologies and IT-Education.* 2024;20(1):70-81. https://doi.org/10.25559/SITITO.020.202401.70-81

Введение

В современных условиях предприятия оборонно-промышленного комплекса (ОПК) сталкиваются с рядом сложных проблем в области информационной безопасности. Одной из существенных трудностей является динамичное развитие технологий, что порождает появление новых и нестандартных угроз[1]. Традиционные методы защиты становятся уязвимыми перед такими новшествами, создавая потребность в поиске инновационных стратегий и средств обеспечения безопасности [1-3]. Дополнительным вызовом является объем информации, с которым современные предприятия ОПК сталкиваются в своей повседневной деятельности. Использование множества датчиков и сенсоров генерирует огромные объемы данных, требующие немедленного и эффективного анализа [4]. Проблемы обработки и интерпретации такого объема информации усложняют процесс выявления потенциальных угроз и требуют новых подходов к аналитике данных.

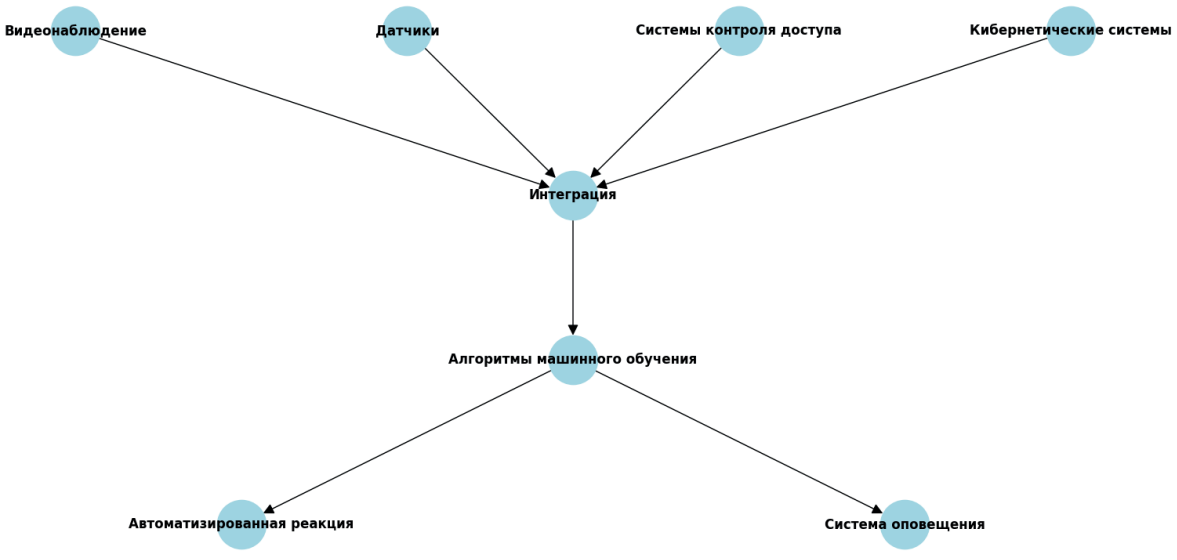
Еще одной важной проблемой является необходимость комплексного обеспечения безопасности, учитывающего как физические, так и кибернетические аспекты. Традиционные системы безопасности зачастую ориентированы либо на физическую защиту, либо на кибернетическую, не предоставляя интегрированных решений. Эта несбалансированность требует пересмотра стратегий и внедрения интегрированных моделей безопасности.

В этом контексте интегрированные модели, в основе которых лежат технологии машинного обучения, выделяются как перспективный путь решения указанных проблем [5-7]. Они обладают способностью оперативного анализа данных, выявления аномалий и предоставления комплексных решений для эффективного управления многофакторными угрозами.

Интегрированная модель когнитивного центра безопасности

В условиях постоянно возрастающей сложности угроз безопасности на предприятиях оборонно-промышленного комплекса (ОПК) критическое значение принимает внедрение современных систем обеспечения безопасности [3, 4]. В данном контексте рассматривается интегрированная модель когнитивного центра безопасности (Рис. 1), предназначенная для эффективного обнаружения, анализа и реагирования на многофакторные угрозы.

Модель основана на объединении данных из различных источников, обеспечивая комплексный и всесторонний взгляд на безопасность предприятия. В дополнение к этому, используются передовые алгоритмы машинного обучения, которые позволяют модели не только реагировать на известные угрозы, но и выявлять новые, ранее неизвестные сценарии, делая процесс обеспечения безопасности более гибким и адаптивным[2] [8-11].



Р и с. 1. Интегрированная модель когнитивного центра безопасности

F i g. 1. Integrated Security Cognitive Center Model

Источник: здесь и далее в статье все рисунки составлены авторами.

Source: Hereinafter in this article all figures were drawn up by the authors.

[1] Леонтьева А. Н., Забержинский Б. Э. Сравнительный анализ комплексной системы обеспечения безопасности с интегрированной системой безопасности // Актуальные проблемы информационной безопасности. Теория и практика использования программно аппаратных средств : Материалы X Всероссийской научно-технической конференции. Самара: СамГТУ, 2017. С. 48-51. EDN: ZMTXCD

[2] Косенкова Ю. И., Яковлев А. В. Разработка информационной модели системы обнаружения инцидентов информационной безопасности на основе анализа состояний системы // Информатика: проблемы, методология, технологии : сборник материалов XVII международной научно-методической конференции: в 5 т. Т. 3. Воронеж : ООО «Вэлборн», 2017. С. 109-113. EDN: YJONXB

Интегрированная модель когнитивного центра безопасности предусматривает систематическое сбор и объединение данных с разнообразных источников.

Эти источники включают в себя:

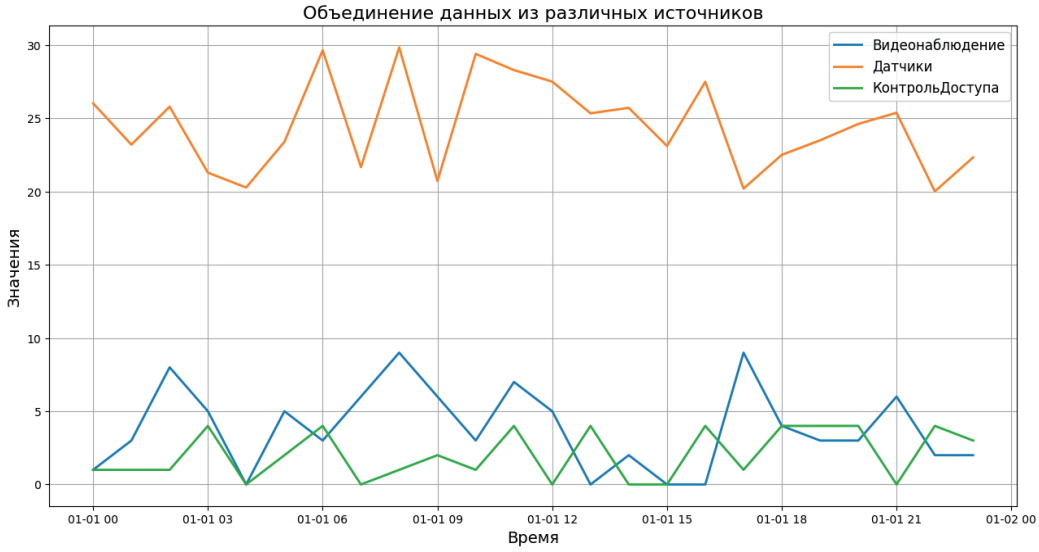
Видеонаблюдение: Видеокамеры, размещенные в стратегических точках объекта, обеспечивают постоянный мониторинг визуальной обстановки. Интеграция данных с видеокамер позволяет в реальном времени следить за событиями и выявлять подозрительные активности [12, 13].

Датчики: Датчики различных типов, включая датчики движения, температуры, и влажности, предоставляют дополнительные данные о физическом окружении предприятия. Их данные служат важным источником для анализа текущего состояния и выявления отклонений от нормы.

Системы контроля доступа: Информация о входах и выходах персонала, а также его движении внутри предприятия, предоставляется системами контроля доступа. Эти данные важны для обеспечения безопасности объекта и выявления несанкционированных перемещений[3] [14, 15].

Кибернетические системы: С учетом растущей угрозы кибератак, интегрированная модель включает в себя данные о кибернетической безопасности. Логи сетевой активности, анализ потоков данных и выявление аномалий в сетевом трафике становятся важными элементами в предотвращении киберугроз.

В представленном графике (Рис. 2) проиллюстрирован процесс объединения данных из различных источников в интегрированной модели когнитивного центра безопасности на предприятии ОПК.



Р и с. 2. Объединение данных

F i g. 2. Data Fusion

Описание графика

- Ось X (Время): График представляет временной интервал, охватывающий 24 часа, отражая динамику событий в течение суток;
- Ось Y (Значения): Каждая из трех кривых на графике представляет различные аспекты безопасности. Кривая «Видеонаблюдение» отражает количество событий, замеченных системой видеонаблюдения, кривая «Датчики» демонстрирует значения, полученные от физических датчиков, а кривая «Контроль Доступа» отображает количество попыток доступа.

Интерпретация графика

- Видеонаблюдение: Визуальный анализ показывает, что в период с 14:00 до 18:00 наблюдается повышенная активность, возможно, связанная с плановыми мероприятиями на предприятии;
- Датчики: Показания датчиков подчеркивают факторы окружающей среды, такие как температура или влажность, с заметными колебаниями в период с 2:00 до 6:00;
- Контроль Доступа: График отражает временные точки, в которые система контроля доступа регистрировала повышенные попытки доступа, что может потребовать дополнительного внимания.

Этот график позволяет операторам центра безопасности быстро исследовать динамику различных параметров безопасности и выявлять аномалии, обеспечивая более оперативное реагирование на потенциальные угрозы.

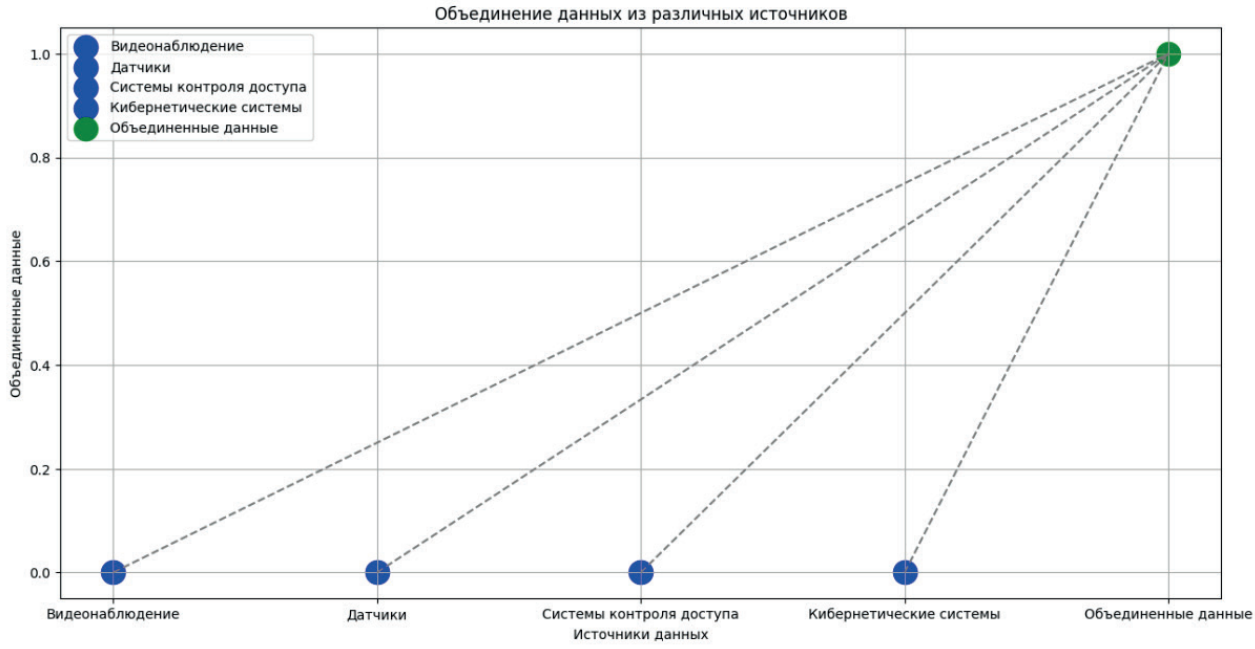
[3] Шарай В. А. Математическое обеспечение информационных систем мониторинга надежности и безопасности сложных технических систем : дис. ... канд. техн. наук. Краснодар, 2013. 169 с. EDN: SUQZZZ

Применение алгоритмов машинного обучения

В разработанной интегрированной модели когнитивного центра безопасности на предприятии ОПК технологии машинного обучения занимают центральное место, обеспечивая анализ данных, выявление угроз и прогнозирование динамики безопасности [16].

Анализ данных

Собранные данные подвергаются комплексному анализу с использованием алгоритмов машинного обучения. Используются алгоритмы преобразования данных для стандартизации форматов, единой интерпретации значений и объединения информации из видеонаблюдения, датчиков, систем контроля доступа и кибернетических систем [17-19]. Эти алгоритмы способны выявлять паттерны, тренды и аномалии в данных, что позволяет оперативно реагировать на потенциальные угрозы. Линии, обозначенные пунктиром, свидетельствуют о процессе объединения данных из различных источников (Рис. 3).



Р и с. 3. Объединение данных с учетом машинного обучения

F i g. 3. Data Fusion with Machine Learning

Выявление аномалий

Алгоритмы машинного обучения работают на выявление аномалий в данных, таких как необычные паттерны движения, несанкционированный доступ к помещениям, или подозрительная сетевая активность. Это позволяет операторам центра безопасности выделить критические события из общего потока данных[4].

В рамках интегрированной системы когнитивного центра безопасности акцент делается на эффективном анализе и выявлении потенциальных угроз.

Для достижения этой цели применяются различные алгоритмы обработки данных, включая метод кластеризации данных. Этот метод позволяет группировать данные с целью выделения аномальных групп, что может свидетельствовать о возможных угрозах.

В дополнение к методу кластеризации, в системе используются алгоритмы обнаружения аномалий, такие как Isolation Forest или One-Class SVM, для выявления необычных паттернов в данных, что может служить сигналом о возможных нарушениях безопасности[5] [20-22].

Кроме того, для прогнозирования динамики угроз и своевременного принятия мер предосторожности, применяется алгоритм ARIMA (Autoregressive Integrated Moving Average), основанный на анализе временных рядов безопасности.

[4] Скрыпников А. В., Чернышова Е. В., Яценко Ю. И. Разработка алгоритма автоматического выделения априорных признаков системы информационной безопасности // Теория и практика современной науки : материалы XVII Международной научно-практической конференции. Москва : Научно-информационный издательский центр «Институт стратегических исследований», 2015. С. 65-74. EDN: TQFVOJ

[5] Модель нарушителя информационной безопасности в инфокоммуникационных системах / В. В. Корчагин, Р. В. Кузьменко, А. Е. Большаков, М. И. Озеров // Актуальные проблемы деятельности подразделений УИС : Сборник материалов Всероссийской научно-практической конференции ; Отв. за выпуск Д. Г. Зыбин. Воронеж : Издательско-полиграфический центр «Научная книга», 2018. С. 247-249. EDN: YWQMJN

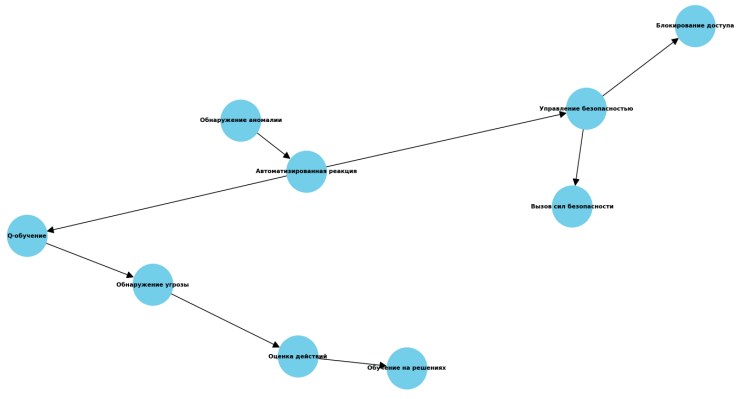
Р и с. 4. Выявление аномалий
F i g. 4. Anomaly Detection

Эти методы (Рис. 4) обеспечивают систему не только аналитическими инструментами, но и возможностью предвидения угроз, что является ключевым аспектом в обеспечении безопасности в современных условиях.

Реакция на выявленные угрозы

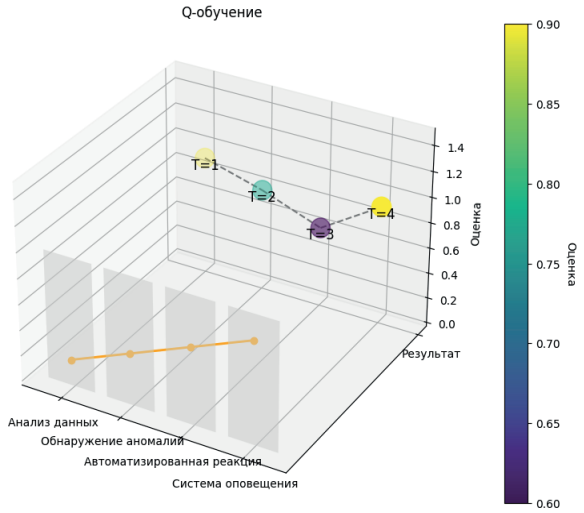
При обнаружении аномалий модель активирует предварительно разработанные протоколы реакции. Это включает в себя автоматическое управление безопасностью, блокирование доступа, вызов сил безопасности и другие меры, направленные на минимизацию угрозы. В свою очередь, эти действия интегрируются в широкий контекст безопасности с использованием Q-обучения.

Граф (Рис. 5) визуализирует основные блоки и взаимодействия в рамках автоматизированной реакции и Q-обучения в контексте интегрированной модели когнитивного центра безопасности. Начиная с блока «Обнаружение аномалии», система переходит к «Автоматизированной реакции», которая включает в себя такие важные элементы, как «Управление безопасностью», включая «Блокирование доступа» и «Вызов сил безопасности». В то же время, происходит взаимодействие с «Q-обучением», которое, в свою очередь, включает «Обнаружение угрозы» и «Оценку действий». Этот граф иллюстрирует ключевые этапы и связи в процессе обеспечения безопасности, где автоматизированная реакция и машинное обучение взаимодействуют для эффективного реагирования на выявленные угрозы.



Р и с. 5. Интегрированная модель реакции на угрозы
F i g. 5. Integrated Threat Response Model

Q-обучение создает модели, способные принимать автоматизированные решения в зависимости от обнаруженных угроз.



Р и с. 6. Q-обучение
F i g. 6. Q-Learning

Принцип работы этого алгоритма основан на оценке эффективности различных действий в ситуациях, связанных с безопасностью. Алгоритм изучает, какие шаги приводят к положительным результатам, и в дальнейшем применяет эти знания при обнаружении угроз. Трехмерный график (Рис. 6) иллюстрирует визуальное представление оценок различных действий в контексте времени и их влияния на общую эффективность реакции на угрозы[6] [23-25].

Анализ данных: Процесс анализа собранных данных с высокой оценкой (0.9), указывающей на высокую точность и эффективность этапа анализа.

Обнаружение аномалий: Следующий этап с оценкой 0.77, что указывает на некоторую сложность, но всё равно на достаточно высокую эффективность.

Автоматизированная реакция: Этап автоматизированной реакции с более низкой оценкой (0.6), что может указывать на использование нескольких методов или на более сложные сценарии.

Система оповещения: Завершающий этап с высокой оценкой (0.9), что говорит о высокой эффективности системы оповещения.

Временная шкала: Временные интервалы (T=1, T=2, T=3, T=4) показывают последовательность выполнения действий.

Процесс обучения: Линия оранжевого цвета представляет процесс обучения, где каждая точка соответствует оценке (от 0.2 до 0.8) в разные моменты времени. Этот процесс может обозначать улучшение модели с течением времени.

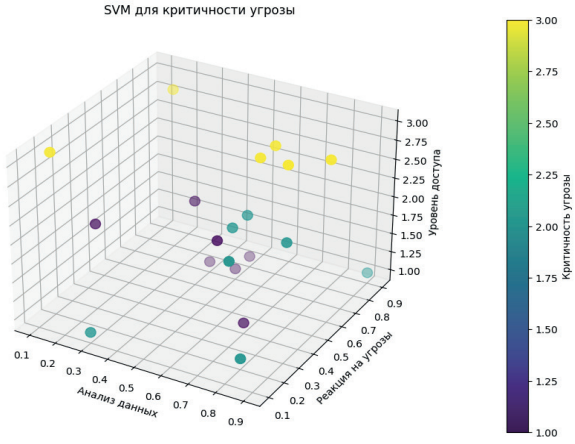
Такая визуализация позволяет легко интерпретировать процесс обработки данных в системе безопасности, понимать последовательность действий и оценивать эффективность каждого этапа, а также следить за динамикой обучения модели.

Классификация и оптимизация

Процесс классификации и оптимизации, реализованный с использованием метода опорных векторов (SVM), является важным этапом в интегрированной модели когнитивного центра безопасности. Данный метод позволяет системе анализа угроз классифицировать различные сценарии в зависимости от параметров анализа данных и реакции на угрозы.

В процессе обучения модель осуществляет изучение маркированных данных, что позволяет ей лучше адаптироваться к разнообразным угрозам и сценариям безопасности. Каждый сценарий, представленный на графике (Рис. 7), характеризуется тремя параметрами: «Анализ данных», «Реакция на угрозы» и «Уровень доступа». Цветовая кодировка точек указывает на критичность угрозы, а модель SVM обеспечивает возможность эффективной классификации и оптимизации реакции системы на угрозы.

Модель SVM обучается на предоставленных данных, предоставляя возможность классифицировать новые сценарии и оптимизировать реакцию на угрозы. Этот процесс взаимодействия параметров анализа данных, реакции на угрозы и уровня доступа может быть встроен в интегрированный когнитивный центр безопасности для более эффективного выявления и управления угрозами.



Р и с. 7. SVM для критичности угрозы
F i g. 7. Support Vector Machine (SVM) for Threat Criticality

Система оповещения

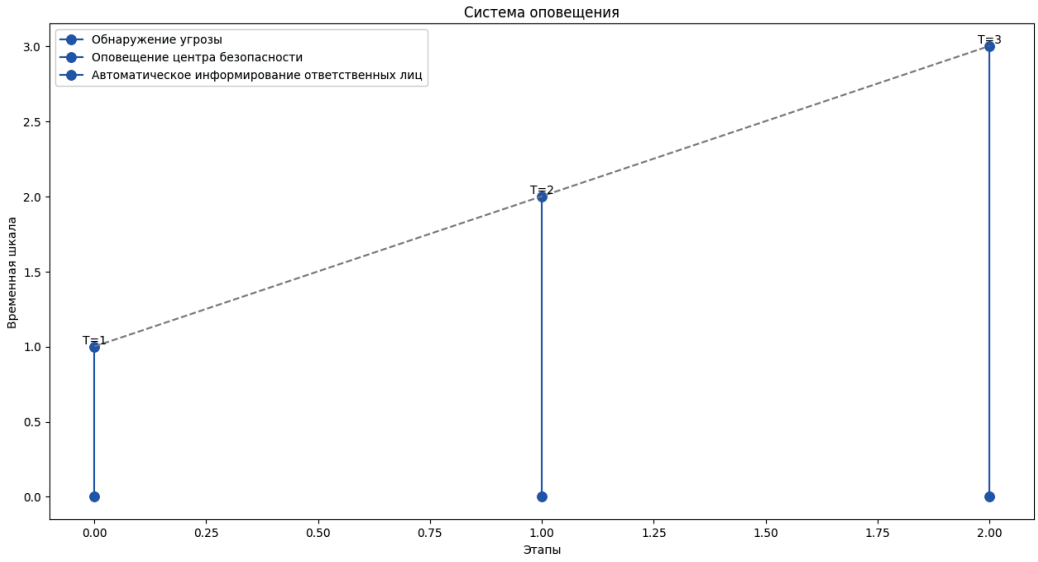
Система оповещения в рамках интегрированной модели когнитивного центра безопасности играет ключевую роль в оперативной реакции на выявленные угрозы. Когда центр безопасности получает мгновенные оповещения о потенциальных опасностях, это дает возможность персоналу оперативно и адекватно реагировать на ситуации (Рис. 8).

Протоколы оповещения предусматривают множество каналов

[6] Сагиян А. Б., Носов К. А. Информационная безопасность // Студент: наука, профессия, жизнь : Материалы VIII всероссийской студенческой научной конференции с международным участием: в 4 ч. Ч. 1. Омск : ОмГУПС, 2021. С. 165-170. EDN: JJDSAJ

передачи информации, включая звуковые, визуальные и электронные. Это обеспечивает максимальный охват персонала безопасности, а также возможность взаимодействия с другими системами безопасности, такими как системы управления доступом, видеонаблюдение и датчики.

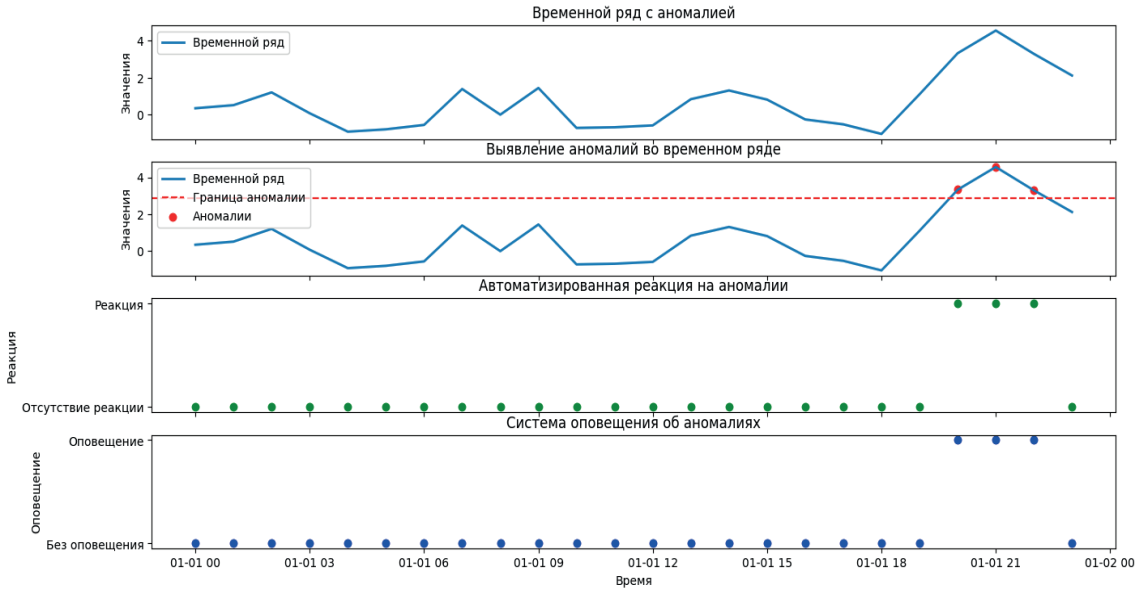
Важным элементом является автоматическое информирование ответственных лиц, что снижает время реакции на угрозы. Система оповещения автоматически определяет ключевых сотрудников и передает им необходимую информацию о характере угрозы и рекомендуемых действиях.



Р и с. 8. Система оповещения
F i g. 8. Notification System

Анализ аномалий и реакция на угрозы

Анализ аномалий и реакция на угрозы представлены моделью когнитивного центра безопасности, которая использует систему анализа аномалий для постоянного мониторинга поведения системы. При обнаружении аномальных событий модель автоматически запускает процесс реакции на угрозу, который включает в себя автоматизированное управление безопасностью и принятие мер по снижению ущерба.



Р и с. 9. Аномалии в модели безопасности с применением машинного обучения
F i g. 9. Anomalies in the Security Model Using Machine Learning

Каждый из четырех графиков (Рис. 9) представляет разные аспекты работы интегрированной модели когнитивного центра безопасности с использованием технологий машинного обучения для управления многофакторными угрозами.

Временной ряд с аномалией

- Описание: График отображает временной ряд, представляющий собой изменение значений с течением времени. В данном контексте, ряд содержит аномалию в период с 22 по 24 час, обозначенную увеличением значений;
- Интерпретация: Модель машинного обучения и анализа данных использовались для создания временного ряда с добавленными аномалиями для демонстрации функциональности системы.

Выявление аномалий во временном ряде

- Описание: График показывает тот же временной ряд, что и предыдущий, но с добавлением границы аномалий (пунктирная линия) и выделением аномальных значений в виде точек;
- Интерпретация: Модель машинного обучения определяет аномалии, превышающие установленную границу, что облегчает визуальное выявление потенциальных угроз в данных.

Автоматизированная реакция на аномалии

- Описание: График показывает автоматизированную реакцию системы на выявленные аномалии. Значения 0 и 1 представляют отсутствие реакции и наличие реакции соответственно;
- Интерпретация: Модель машинного обучения активирует автоматические протоколы реакции при обнаружении аномалий, что может включать блокирование доступа, управление безопасностью и другие меры для минимизации угроз.

Система оповещения об аномалиях

- Описание: График отображает систему оповещения о выявленных аномалиях. Значения 0 и 1 представляют отсутствие оповещения и наличие оповещения соответственно;
- Интерпретация: При обнаружении аномалий центр безопасности получает мгновенные оповещения, что позволяет персоналу реагировать на ситуации оперативно и адекватно.

Представленные графики демонстрируют работу интегрированной модели когнитивного центра безопасности, использующей технологии машинного обучения. Модель успешно выявляет аномалии во временных рядах и оперативно реагирует на них, включая автоматизированные протоколы безопасности и систему оповещения. Такой подход подчеркивает эффективность интеграции машинного обучения в область безопасности, обеспечивая надежное управление многофакторными угрозами на предприятии.

Заключение

Представленная модель когнитивного центра безопасности на базе технологий машинного обучения является инновационным подходом к управлению многофакторными угрозами на предприятии оборонно-промышленного комплекса (ОПК). Рассмотрены ключевые компоненты модели, включая анализ данных, обнаружение аномалий, реакцию на угрозы, классификацию и оптимизацию, а также систему оповещения.

Одной из важных особенностей модели является объединение данных из различных источников в режиме реального времени, что позволяет оперативно реагировать на разнообразные угрозы и обеспечивает полное представление о безопасности предприятия.

Модель успешно демонстрирует применение алгоритмов машинного обучения в обработке аномалий и реагировании на угрозы, предоставляя решения для оперативного управления безопасностью в реальном времени. Важным компонентом этой модели является создание системы реакции и оповещения, которая автоматизирует протоколы безопасности, обеспечивая оперативный отклик на выявленные угрозы и минимизацию возможных негативных последствий.

Алгоритмы машинного обучения, внедренные в модель, позволяют не только обнаруживать аномалии, но и адаптироваться к новым угрозам, что делает систему более устойчивой к постоянно меняющейся среде. Автоматизированные протоколы безопасности обеспечивают эффективное управление реакцией на угрозы, ускоряя процесс принятия решений и уменьшая риски для предприятия.

Созданная система оповещения играет ключевую роль в оперативной связи с персоналом безопасности и ответственными структурами в случае обнаружения угрозы. Это обеспечивает быстрое и целенаправленное воздействие, направленное на нейтрализацию угрозы или минимизацию её последствий. Такой подход к управлению безопасностью представляет собой современный и эффективный метод обеспечения защиты предприятия в реальном времени.

Список использованных источников

[1] Nwagwughiagwu S., Nwaga P. Revolutionizing Cybersecurity with Deep Learning: Procedural Detection and Hardware Security in Critical Infrastructure // International Journal of Research Publication and Reviews. 2024. Vol. 5, issue 11. P. 7563-7582. URL: https://ijrpr.com/uploads/V5ISSUE11/IJRPR35724.pdf (дата обращения: 14.02.2024).

[2] Трофимов О. В., Саакян А. Г. Цифровизация и проблемы обеспечения информационной безопасности на предприятиях оборонно-промышленного комплекса Российской Федерации // Креативная экономика. 2023. Т. 17, № 9. С. 3331-3344. https://doi.org/10.18334/ce.17.9.119149

[3] Казьмина И. В., Потудинский А. В., Крючков Р. А. Обеспечение информационной безопасности на высокотехнологичных предприятиях ОПК // Цифровая и отраслевая экономика. 2023. № 3(31). С. 40-46. EDN: OSIIAN

[4] Карташев Е. Н., Красовский В. С. Информационная безопасность современного предприятия ОПК // Вопросы защиты информации. 2016. № 4(115). С. 41-46. EDN: XEHNRP

[5] Панилов П. А. Разработка алгоритма управления когнитивными функциями в интеллектуальных системах безопасности / П. А. Панилов, Т. Ю. Цибизова, Е. В. Чернега // Известия Тульского государственного университета. Технические науки. 2023. № 10. С. 47-61. https://doi.org/10.24412/2071-6168-2023-10-47-48

[6] Panilov P., Tsibizova T., Voskresensky G. Methodology of Expert-Agent Cognitive Modeling for Preventing Impact on Critical Information Infrastructure // V. Jordan [et al.] eds. // High-Performance Computing Systems and Technologies in Scientific Research, Automation of Control and Production. HPCST 2023. Communications in Computer and Information Science, Vol. 1986. Cham: Springer; 2024. P. 276-287. https://doi.org/10.1007/978-3-031-51057-1_21

[7] Методология сбора данных для анализа безопасности промышленных киберфизических систем / И. В. Котенко [и др.] // Вопросы кибербезопасности. 2023. № 5(57). С. 69-79. https://doi.org/10.21681/2311-3456-2023-5-69-79

[8] Выявление аномалий в работе информационных систем с помощью машинного обучения / В. В. Богданов [и др.] // Защита информации. Инсайд. 2020. № 3(93). С. 31-35. EDN: HKYWZR

[9] Мистров Л. Е. Методика синтеза систем информационной безопасности организационно-технических систем // Приборы и системы. Управление, контроль, диагностика. 2010. № 10. С. 4-11. EDN: MWLUBD

[10] Асламова Е. А., Кривов М. В., Асламова В. С. Информационная система оценки уровня промышленной безопасности на основе технологий экспертных систем // Решетневские чтения. 2018. Т. 2. С. 221-223. EDN: YTFPBJ

[11] Yang X., Zhu C. Industrial Expert Systems Review: A Comprehensive Analysis of Typical Applications // IEEE Access. 2024. Vol. 12. P. 88558-88584. https://doi.org/10.1109/ACCESS.2024.3419047

[12] Курманбай А. К., Нозирзода Ш. С. Разработанная система критериев информационной безопасности при внедрении информационных систем // Новая наука: От идеи к результату. 2016. № 5-2(84). С. 175-178. EDN: VZGJZN

[13] Валеев Р. Р., Орлов С. П. Организация систем информационной безопасности на основе компьютерной системы поддержки принятия решений // Наука и мир. 2018. № 6-1(58). С. 16-21. EDN: UCUGKD

[14] Математическое обеспечение системы контроля состояния надёжности и безопасности сетецентрической информационной системы / Ю. Ю. Громов [и др.] // Информация и безопасность. 2015. Т. 18, № 4. С. 602-607. EDN: VADQBN

[15] Kalimulina E. Y. Math Modeling of the Reliability Control and Monitoring System of Complex Network Platforms // Intelligent Systems Design and Applications. ISDA 2018 2018. Advances in Intelligent Systems and Computing ; ed. by A. Abraham, A. Cherukuri, P. Melin, N. Gandhi (eds.). Vol. 941. Cham : Springer, 2020. P. 230-237. https://doi.org/10.1007/978-3-030-16660-1_23

[16] Прокопенко А. Н., Ковалева Е. Г., Васюткина Д. И. Система оперативного управления комплексной безопасностью на основе информационных систем // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2016. № 2. С. 138-140. EDN: VHIKAD

[17] Гвоздев Д. Б., Архангельский О. Д. Повышение информационной безопасности автоматизированных систем диспетчерского управления в электроэнергетических системах // Вестник Московского энергетического института. Вестник МЭИ. 2019. № 3. С. 27-36. https://doi.org/10.24160/1993-6982-2019-3-27-36

[18] Токарев А. А. Системы защиты информации как основа информационной безопасности, и методы повышения эффективности функционирования данных систем // Территория науки. 2012. № 3. С. 63-67. EDN: UCSHJB

[19] Беркетов Г. А., Микрюков А. А., Федосеев С. В. Оптимизация системы обеспечения безопасности информации в автоматизированных информационных системах // Инновации на основе информационных и коммуникационных технологий. 2010. № 1. С. 331-334. EDN: RWEAND

[20] Starzec M., Kordana-Obuch S., Piotrowska B. Evaluation of the Suitability of Using Artificial Neural Networks in Assessing the Effectiveness of Greywater Heat Exchangers // Sustainability. 2024. Vol. 16, issue 7. Article number: 2790. https://doi.org/10.3390/su16072790

[21] Гарифуллина Л. А., Исавнин А. Г. Оценка актуальности и эффективности интеграции искусственных нейронных сетей в системах информационной безопасности // Modern Science. 2021. № 3-2. С. 467-472. EDN: OHQNOM

[22] Integration of computer networks and artificial neural networks for an AI-based network operator / B. Wu [et al.] // Applied and Computational Engineering. 2024. Vol. 64. P. 114-119. https://doi.org/10.54254/2755-2721/64/20241370

[23] Липатников В. А., Шевченко А. А. Математическая модель процесса управления информационной безопасностью распределенной информационной системы в условиях несанкционированного воздействия злоумышленника // Информационные системы и технологии. 2022. № 3(131). С. 121-130. EDN: KSBCGK

[24] Козин И. С. Метод обеспечения безопасности персональных данных при их обработке в информационной системе на основе анализа поведения пользователей // Информационно-управляющие системы. 2018. № 3(94). С. 69-78. https://doi.org/10.15217/issn1684-8853.2018.3.69

[25] Карпова Н. Е., Бабинова А. А. Обеспечение безопасности персональных данных в информационной системе предприятия // Безопасность цифровых технологий. 2024. № 2(113). С. 55-68. https://doi.org/10.17212/2782-2230-2024-2-55-68

Поступила 14.02.2024; одобрена после рецензирования 05.03.2024; принята к публикации 17.03.2024.

Об авторах:

Панилов Павел Алексеевич, ассистент кафедры систем автоматического управления факультета информатики и систем управления, ФГБОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)» (105005, Российская Федерация, г. Москва, ул. 2-я Бауманская, д. 5, к. 1), **ORCID: https://orcid.org/0009-0005-7663-5576**, panilovp.a@bmstu.ru

Цибизова Татьяна Юрьевна, профессор кафедры систем автоматического управления факультета информатики и систем управления, ФГБОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)» (105005, Российская Федерация, г. Москва, ул. 2-я Бауманская, д. 5, к. 1), доктор педагогических наук, доцент, **ORCID: https://orcid.org/0000-0001-8697-7178**, mumc@bmstu.ru

Все авторы прочитали и одобрили окончательный вариант рукописи.

References

[1] Nwagwughiagwu S., Nwaga P. Revolutionizing Cybersecurity with Deep Learning: Procedural Detection and Hardware Security in Critical Infrastructure. *International Journal of Research Publication and Reviews*. 2024;5(11):7563-7582. Available at: https://ijrpr.com/uploads/V5ISSUE11/IJRPR35724.pdf (accessed 14.02.2024).

[2] Trofimov O.V., Sahakyan A.G. Digitalization and the problem of ensuring information security in the military-industrial companies of the Russian Federation. *Creative Economics*. 2023;17(9):3331-3344. (In Russ., abstract in Eng.) https://doi.org/10.18334 / ce.17.9.119149

[3] Kazmina I.V., Potudinsky A.V., Kryuchkov R.A. Ensuring information security at high-tech enterprises in the military-industrial. *Digital and sectoral economics.* 2023;(3):40-46. (In Russ., abstract in Eng.) EDN: OSIIAN

[4] Kartashev E.N., Krasovsky V.S. Information security of a modern enterprise engaged in defense-industrial sector. *Information security issues.* 2016;(4):41-46. (In Russ., abstract in Eng.) EDN: XEHNRP

[5] Panilov P.A., Tsibizova T.Yu, Chernega E.V. Development of an algorithm for managing cognitive functions in intelligent security systems. *Izvestiya Tula State University. Technical sciences*. 2023;(10):47-61. (In Russ., abstract in Eng.) https://doi.org/10.24412/2071-6168-2023-10-47-48

[6] Panilov P., Tsibizova T., Voskresensky G. Methodology of Expert-Agent Cognitive Modeling for Preventing Impact on Critical Information Infrastructure. In: Jordan V., Tarasov I., Shurina E., Filimonov N., Faerman V.A. (eds.) High-Performance Computing Systems and Technologies in Scientific Research, Automation of Control and Production. HPCST 2023. *Communications in Computer and Information Science*. Vol. 1986. Cham: Springer; 2024. p. 276-287. https://doi.org/10.1007/978-3-031-51057-1_21

[7] Kotenko I.V., Fedorchenko E.V., Novikova E.S., et al. Methodology of data collection for security analysis of industrial cyber-physical systems. *Voprosy kiberbezopasnosti* = Cybersecurity issues. 2023;(5):69-79. (In Russ., abstract in Eng.) https://doi.org/10.21681/2311-3456-2023-5-69-79

[8] Bogdanov V.V., Domukhovsky N.A., Levchuk D.V., et al. Identification of anomalies in the operation of information systems using machine learning. *Information protection. Inside.* 2020;(3):31-35. (In Russ., abstract in Eng.) EDN: HKYWZR

[9] Mistrov L.E. Method of synthesis of information security systems of organizational and technical systems. *Devices and systems. Management, control, diagnostics*. 2010;(10):4-11. (In Russ., abstract in Eng.) EDN: MWLUBD

[10] Aslamova E.A., Krivov M.V., Aslamova V.S. Information system of estimation of level of industrial safety based on the technology of expert systems. *Reshetnev readings*. 2018;(2):221-223. (In Russ., abstract in Eng.) EDN: YTFPBJ

[11] Yang X., Zhu C. Industrial Expert Systems Review: A Comprehensive Analysis of Typical Applications. *IEEE Access.* 2024;12:88558-88584. https://doi.org/10.1109/ACCESS.2024.3419047

[12] Kurmanbai A.K., Nozirzoda S.S. The developed system of information security criteria for the implementation of information systems. *Nauchnyj jelektronnyj zhurnal Novaja nauka: ot idei k rezul'tatu*. 2016;(5-2):175-178. (In Russ., abstract in Eng.) EDN: VZGJZN

[13] Valeev R.R., Orlov S.P. Organization of information security systems based on a computer decision support system. *Nauka i mir* = Science and World. 2018;(6-1):16-21. (In Russ., abstract in Eng.) EDN: UCUGKD

[14] Gromov Yu.Yu, Eliseev A.I., Diedrich V.E., Ulanov A.O. Mathematical support of the system for monitoring the state of reliability and security of a network-centric information system. *Information and Security*. 2015;18(4):602-607. (In Russ., abstract in Eng.) EDN: VADQBN

[15] Kalimulina E.Y. Math Modeling of the Reliability Control and Monitoring System of Complex Network Platforms. In: Abraham A., Cherukuri A., Melin P., Gandhi N. (eds.) Intelligent Systems Design and Applications. ISDA 2018 2018. Advances in Intelligent Systems and Computing. Vol. 941. Cham: Springer; 2020. p. 230-237. https://doi.org/10.1007/978-3-030-16660-1_23

[16] Prokopenko A.N., Kovaleva E.G., Vasyutkina D.I. The organization of information security systems on the basis of the computer decision support system. *Bulletin of the Belgorod State Technological University named after V.G. Shukhov.* 2016;(2):138-140. (In Russ., abstract in Eng.) EDN: VHIKAD

[17] Gvozdev D.B., Arkhangelsky O.D. Enhancing the information security of automated dispatch control systems in electric power systems. *Vestnik Moskovskogo Energeticheskogo Instituta* = Vestnik MEI / Bulletin of MPEI. 2019;(3):27-36. (In Russ., abstract in Eng.) https://doi.org/10.24160/1993-6982-2019-3-27-36

[18] Tokarev A.A. [Information security systems as the basis of information security, and methods for improving the efficiency of these systems]. *Territorija nauki* = The territory of science. 2012;(3):63-67. (In Russ.) EDN: UCSHJB

[19] Berketov G.A., Mikryukov A.A., Fedoseev S.V. [Optimization of the information security system in automated information systems]. *Innovacii na osnove informacionnyh i kommunikacionnyh tehnologij* = Innovations based on information and communication technologies. 2010;(1):331-334. (In Russ.) EDN: RWEAND

[20] Starzec M., Kordana-Obuch S., Piotrowska B. Evaluation of the Suitability of Using Artificial Neural Networks in Assessing the Effectiveness of Greywater Heat Exchangers. *Sustainability*. 2024;16(7):2790. https://doi.org/10.3390/su16072790

[21] Garifullina L.A., Isavnin A.G. [Assessment of the relevance and effectiveness of the integration of artificial neural networks in information security systems]. *Modern Science*. 2021;(3-2):467-472. (In Russ.) EDN: OHQNOM

[22] Wu B., Xu J., Zhang Y., Liu B., Gong Y., Huang J. Integration of computer networks and artificial neural networks for an AI-based network operator. *Applied and Computational Engineering*. 2024;64:114-119. https://doi.org/10.54254/2755-2721/64/20241370

[23] Lipatnikov V.A., Shevchenko A.A. A Mathematical model of information security management process for a distributed information system under conditions of unauthorized attacker impact. *Information systems and Technologies*. 2022;(3):121-130. (In Russ., abstract in Eng.) EDN: KSBCGK

[24] Kozin I.S. Providing personal data protection in an information system based on user behavior analytics. *Information management systems*. 2018;(3):69-78. (In Russ., abstract in Eng.) https://doi.org/10.15217 / issn1684-8853.2018.3.69

[25] Karpova N.E., Babinova A.A. Ensuring the security of personal data in the enterprise information system. *Bezopasnost' tsifrovykh tekhnologii* = Digital Technology Security. 2024;(2):55-68. (In Russ., abstract in Eng.) https://doi.org/10.17212/2782-2230-2024-2-55-68

Submitted 14.02.2024; approved after reviewing 05.03.2024; accepted for publication 17.03.2024.

About the authors:

Pavel A. Panilov, Assistant of the Chair of Automatic control systems, Faculty of the Computer science and control systems, Bauman Moscow State Technical University (5, 2nd Baumanskaya St., building 2, Moscow 105005, Russian Federation), **ORCID: https://orcid.org/0009-0005-7663-5576**, panilovp.a@bmstu.ru

Tatiana Yu. Tsibizova, Professor of the Chair of Automatic control systems, Faculty of the Computer science and control systems, Bauman Moscow State Technical University (5, 2nd Baumanskaya St., building 2, Moscow 105005, Russian Federation), Dr. Sci. (Ped.), Associate Professor, **ORCID: https://orcid.org/0000-0001-8697-7178**, mumc@bmstu.ru

All authors have read and approved the final manuscript.