УДК 004.8:351.862

Рыспаев Рауан Серикович

ТОО «Дельта Групп Астана» / Астана, Казахстан

Генеральный директор

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ СИТУАЦИОННОГО АНАЛИЗА В КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ

Аннотация: *В статье исследуются подходы к применению интеллектуальных систем ситуационного анализа для обеспечения комплексной безопасности объектов. Рассматриваются принципы интеграции технологий искусственного интеллекта, машинного обучения и обработки больших данных в процессы выявления аномалий и прогнозирования угроз. Проанализированы архитектура и алгоритмы систем, основанных на корреляции событий и оценке рисков в реальном времени. Особое внимание уделено вопросам точности данных, прозрачности алгоритмов и этическим аспектам автоматизированных решений. Показано, что использование интеллектуальных систем позволяет перейти от реактивной к проактивной модели управления рисками, повышая устойчивость инфраструктуры и снижая зависимость от человеческого фактора. Сделан вывод, что дальнейшее развитие таких технологий требует нормативной базы, обеспечивающей баланс между инновациями, безопасностью и ответственностью.*

Ключевые слова: *интеллектуальные системы; ситуационный анализ; комплексная безопасность; машинное обучение; анализ данных; прогнозирование угроз; кибербезопасность; автоматизация.*

Rauan Serikovich Ryspayev
LLP "Delto Group Astana" / Astana, Kazakhstan
Chief Executive Officer

INTELLIGENT SYSTEMS OF SITUATIONAL ANALYSIS IN THE COMPREHENSIVE SECURITY OF FACILITIES

Abstract: *The article examines approaches to the use of intelligent situational analysis systems to ensure the comprehensive security of facilities. It discusses the principles of integrating artificial intelligence, machine learning, and big data processing technologies into processes for detecting anomalies and predicting threats. The architecture and algorithms of systems based on event correlation and real-time risk assessment are analyzed. Particular attention is given to data accuracy, algorithm transparency, and the ethical aspects of automated decision-making. It is shown that the use of intelligent systems enables a transition from a reactive to a proactive risk management model, increasing infrastructure resilience and reducing dependence on the human factor. The conclusion emphasizes that the further development of such technologies requires a regulatory framework that ensures a balance between innovation, security, and accountability.*

Keywords: *intelligent systems; situational analysis; comprehensive security; machine learning; data analysis; threat prediction; cybersecurity; automation.*

Введение

В условиях растущей сложности инфраструктурных систем и увеличения числа потенциальных угроз обеспечение комплексной безопасности объектов становится одной из приоритетных задач современного управления. Традиционные методы, основанные на

разрозненных сенсорных системах и человеческом анализе, уже не обеспечивают необходимую скорость реакции и полноту оценки рисков. Переход к цифровым моделям безопасности требует использования интеллектуальных систем, способных не только фиксировать, но и прогнозировать инциденты, формируя проактивную стратегию защиты [1].

Ключевое направление этой трансформации — развитие систем ситуационного анализа (*situation analysis systems*), основанных на технологиях искусственного интеллекта, машинного обучения и корреляционной аналитики. Такие решения объединяют данные видеонаблюдения, контроля доступа, IoT-датчиков и корпоративных систем, создавая целостное представление об обстановке и повышая оперативность управления.

Интеллектуальные алгоритмы позволяют выявлять аномалии, классифицировать события по уровню риска и формировать оптимальные сценарии реагирования, обеспечивая переход от реактивной к превентивной модели безопасности. Вместе с тем их внедрение сопряжено с технологическими и этическими вызовами — достоверностью данных, прозрачностью алгоритмов и ответственностью за автоматизированные решения [2].

Цель статьи — проанализировать возможности и ограничения интеллектуальных систем ситуационного анализа, рассмотреть используемые алгоритмы и определить перспективы их развития в контексте комплексной безопасности объектов.

1. Эволюция концепции ситуационного анализа в системах безопасности

Понятие ситуационного анализа в сфере безопасности возникло как ответ на необходимость рассматривать не отдельные инциденты, а их взаимосвязь во времени и пространстве. Ранние системы контроля ограничивались регистрацией сигналов тревоги и доступа, а анализ событий проводился постфактум, что снижало эффективность реагирования и не позволяло прогнозировать угрозы.

Развитие ИКТ и интеллектуальных сенсоров сделало возможным переход от дискретного наблюдения к комплексному мониторингу. Концепция *situational awareness*, изначально применявшаяся в военной сфере, была адаптирована для гражданской инфраструктуры — промышленных предприятий, транспортных узлов и энергетики. Её суть заключается в интеграции данных из различных источников и их анализе в реальном времени для формирования целостной картины происходящего.

Современные системы ситуационного анализа строятся на трёх уровнях: обнаружение, оценка контекста и прогнозирование последствий. Такой подход обеспечивает не только реакцию, но и предсказание потенциальных рисков. При этом роль человека меняется: оператор становится контролёром и интерпретатором результатов работы системы, что снижает влияние человеческого фактора и повышает скорость реакции [3].

Внедрение технологий искусственного интеллекта и анализа больших данных позволило автоматизировать обработку потоков информации, превратив системы безопасности из пассивных средств наблюдения в активные инструменты прогнозирования и поддержки решений.

Современный ситуационный анализ представляет собой переход от наблюдения к пониманию, от фиксации событий к управлению рисками, формируя интеллектуальную основу комплексной безопасности объектов.

2. Технологическая основа интеллектуальных систем ситуационного анализа

Современные системы ситуационного анализа опираются на интеграцию технологий искусственного интеллекта, машинного обучения и обработки больших данных. Их задача — объединять разнородные источники информации и обеспечивать автоматическую интерпретацию событий в реальном времени. В отличие от традиционных систем, ориентированных на фиксированные сценарии, интеллектуальные решения обладают адаптивностью и способностью обучаться, повышая точность выявления угроз.

Технологическая архитектура включает несколько уровней: сбор данных от видеокамер, сенсоров доступа, IoT-устройств и сетевых компонентов; интеграцию и очистку данных; аналитическую обработку с применением алгоритмов машинного обучения и корреляции. Алгоритмы кластеризации, классификации и детектирования аномалий анализируют большие объёмы информации, выявляя отклонения от типичного поведения людей, оборудования или сетевой активности. Методы анализа временных рядов позволяют прогнозировать развитие событий и возможные сбои.

Ключевой элемент таких систем — Event Correlation Engine, сопоставляющий информацию из разных источников и определяющий связи между событиями. Это позволяет выявлять сложные сценарии угроз, например, одновременное отключение видеокамеры и несанкционированный доступ.

Результаты анализа отображаются в виде дашбордов, индексов риска и прогнозных графиков, что обеспечивает управляемость и прозрачность. Интеллектуальные системы всё чаще интегрируются с корпоративными платформами — ERP, SCADA, ISMS — и переходят от наблюдения к формированию рекомендаций и автоматическому реагированию.

Технологическая основа интеллектуальных систем ситуационного анализа формирует переход от пассивного мониторинга к активному управлению безопасностью, повышая устойчивость инфраструктуры к внутренним и внешним угрозам.

3. Алгоритмическое выявление аномалий и прогнозирование угроз

Одной из ключевых функций интеллектуальных систем ситуационного анализа является автоматическое выявление аномалий — событий, отклоняющихся от нормального поведения процессов или пользователей. В отличие от пороговых методов, современные алгоритмы используют машинное обучение для построения динамических моделей, способных адаптироваться к изменяющимся условиям и выявлять новые типы угроз без предварительных правил.

Наиболее распространены методы обучения без учителя — кластеризация и поиск выбросов (*k-means*, *DBSCAN*, *Isolation Forest*), которые формируют модель нормального поведения и фиксируют отклонения. При наличии размеченных данных применяются алгоритмы обучения с учителем — деревья решений, случайные леса, нейронные сети, классифицирующие события по уровням риска.

Особое значение имеют гибридные модели, совмещающие статистические методы и нейросети, что позволяет анализировать связи между изменениями параметров среды, доступом, температурой или активностью устройств. На основе таких зависимостей формируется оценка риска (R-Score), определяющая приоритет реагирования.

Применение анализа временных рядов и моделей на основе *LSTM*-сетей позволяет предсказывать вероятность инцидента и переходить от реакции к профилактике. Корреляционные движки (*Event Correlation Engines*) сопоставляют данные из разных источников — видеонаблюдения, контроля доступа, IoT — выявляя контекстные сценарии угроз, например отключение камеры при попытке проникновения.

Эффективность алгоритмического анализа зависит от качества данных и регулярного обновления моделей. Поэтому интеллектуальные системы внедряют *feedback loops*, обучающиеся на собственных ошибках и уменьшающие долю ложных тревог, превращаясь в адаптивный элемент управления безопасностью.

4. Преимущества и ограничения интеллектуальных систем безопасности

Интеллектуальные системы ситуационного анализа стали новым этапом развития комплексной безопасности, позволяя обрабатывать большие объёмы данных в реальном времени и автоматически выявлять угрозы. Они обеспечивают высокую скорость реакции, снижение влияния человеческого фактора и переход к проактивной модели управления рисками.

Использование машинного обучения повышает точность обнаружения инцидентов и сокращает количество ложных тревог.

Интеллектуальные решения объединяют данные из разных источников — видео, контроль доступа, IoT — формируя единый контур безопасности. Это делает возможным предиктивную аналитику и визуализированный контроль эффективности через метрики, такие как IRT, FAR и RME.

Вместе с тем внедрение ИИ в сферу безопасности сопровождается рядом ограничений. Ключевая проблема — зависимость от качества данных: неполные или ошибочные сведения приводят к искажённым результатам. Другой вызов — непрозрачность алгоритмов, когда система выдаёт решения без объяснений, что усложняет аудит и снижает доверие пользователей.

Не менее важно учитывать уязвимость самих интеллектуальных систем: интеграция множества устройств повышает риск кибератак и утечек данных. Кроме того, актуальны этические вопросы — защита персональных данных и распределение ответственности за автоматические решения.

Интеллектуальные системы значительно повышают эффективность и адаптивность защиты, однако требуют строгого контроля, прозрачности и нормативного регулирования для обеспечения устойчивого и ответственного применения.

Заключение

Интеллектуальные системы ситуационного анализа формируют новый стандарт управления безопасностью, основанный на интеграции данных, машинном обучении и аналитике в реальном времени. Они обеспечивают переход от реактивного к проактивному управлению рисками, когда ключевую роль играет не фиксация инцидента, а его прогнозирование и предотвращение.

Использование таких систем повышает точность оценки угроз, снижает нагрузку на персонал и создаёт основу для стратегического управления безопасностью на уровне предприятия или отрасли. Алгоритмическая обработка информации позволяет выявлять скрытые взаимосвязи между событиями и вырабатывать решения быстрее, чем это возможно при ручном анализе.

В то же время развитие интеллектуальных технологий требует строгих стандартов качества данных, прозрачности алгоритмов и этической ответственности за принимаемые решения. Баланс между автоматизацией и человеческим контролем становится ключевым фактором устойчивости и доверия к интеллектуальным системам.

Системы ситуационного анализа с элементами искусственного интеллекта представляют собой не просто инструмент оптимизации, а основу для построения комплексной, адаптивной и предсказуемой архитектуры безопасности, способной соответствовать вызовам цифровой эпохи [4].

Список литературы

1. Артюшкина Е. С., Сафиуллин Д. Ф., Чёрная А. В. ИСПОЛЬЗОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В ЗАЩИТЕ ИНФОРМАЦИИ // Индустриальная экономика. 2023. №4. URL: https://cyberleninka.ru/article/n/ispolzovanie-intellektualnyh-sistem-v-zaschite-informatsii (дата обращения: 10.10.2025).
2. Баранович Андрей Евгеньевич Прагматические аспекты информационной безопасности интеллектуальных систем // История и архивы. 2009. №10. URL: https://cyberleninka.ru/article/n/pragmaticheskie-aspekty-

informatsionnoy-bezopasnosti-intellektualnyh-sistem-1 (дата обращения: 10.10.2025).

3. Табакаева Валерия Александровна, Карманов Игорь Николаевич, Ан Владимир Робертович ОСОБЕННОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ // Интерэкспо Гео-Сибирь. 2020. №2. URL: https://cyberleninka.ru/article/n/osobennosti-intellektualnyh-sistem-upravleniya-informatsionnoy-bezopasnostyu-obektov-kriticheskoy-informatsionnoy-infrastruktury (дата обращения: 10.10.2025).
4. Галанцева К. И. ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ // Форум молодых ученых. 2018. №11-1 (27). URL: https://cyberleninka.ru/article/n/intellektualnye-sistemy-obespecheniya-informatsionnoy-bezopasnosti-2 (дата обращения: 10.10.2025).