РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ОРГАНОВ

Аюбов Рахматулло Равшанбек угли
Ведущий специалист Института макроэкономических и региональных исследований
Ахмедов Турсун Мухитович
Профессор, доктор экономических наук

Аннотация: *В статье рассматриваются актуальные вопросы применения технологий искусственного интеллекта (ИИ) в системах информационной безопасности государственных органов. Анализируются ключевые направления использования ИИ, включая обнаружение киберугроз, управление доступом и автоматизацию реагирования на инциденты. Особое внимание уделяется практическим результатам внедрения и существующим ограничениям.*

Ключевые слова: *искусственный интеллект, информационная безопасность, государственные органы, машинное обучение, киберугрозы, защита данных.*

ВВЕДЕНИЕ

Цифровая трансформация государственного управления неизбежно влечёт за собой расширение поверхности кибератак: государственные органы накапливают колоссальные массивы персональных и служебных данных, управляют критической инфраструктурой и обеспечивают непрерывность публичных услуг. По данным отчёта IBM Security (2023), средняя стоимость утечки данных в государственном секторе составила 2,6 млн долларов США, а среднее время обнаружения инцидента превысило 200 дней. На этом фоне традиционные сигнатурные и правиловые системы защиты утрачивают эффективность против современных адаптивных угроз: целевых атак типа APT, атак на цепочку поставок программного обеспечения и социальной инженерии с использованием deepfake-технологий. Именно поэтому искусственный интеллект становится стратегическим инструментом, позволяющим перейти от реактивной к проактивной модели обеспечения информационной безопасности.

1. Ключевые направления применения ИИ

Применение ИИ в информационной безопасности государственных органов охватывает несколько взаимосвязанных направлений. Первое и наиболее развитое — интеллектуальное обнаружение угроз. Системы класса UEBA (User and Entity Behavior Analytics) на основе методов машинного обучения строят поведенческие профили пользователей и устройств, фиксируя статистически значимые отклонения: нетипичное время входа, необычную географию подключения или резкий рост объёма выгружаемых данных. В отличие от

сигнатурного анализа, такие системы способны выявлять ранее неизвестные угрозы (zero-day) и инсайдерские риски, не поддающиеся обнаружению классическими средствами.

Второе направление — автоматизация реагирования на инциденты посредством платформ SOAR (Security Orchestration, Automation and Response). ИИ-оркестраторы позволяют в течение секунд изолировать скомпрометированный узел, заблокировать учётные записи и запустить форензический сбор доказательств, тогда как аналитик-человек тратил бы на те же действия часы. Третье направление связано с защитой периметра и управлением доступом: алгоритмы компьютерного зрения и поведенческой биометрии обеспечивают непрерывную верификацию личности сотрудников, а ИИ-анализ сетевого трафика позволяет в режиме реального времени выявлять аномальные потоки данных, характерные для эксфильтрации информации или командных серверов вредоносного программного обеспечения.

Таблица 1 — Основные направления применения ИИ в информационной безопасности

Направление	Технология ИИ	Результат применения
Обнаружение угроз	ML-классификаторы	Снижение ложных тревог на 60–70%
Анализ трафика	Нейронные сети	Выявление аномалий в реальном времени
Управление доступом	Поведенческая биометрия	Точность идентификации >98%
Реагирование на инциденты	ИИ-оркестраторы	Сокращение времени реакции в 3–5 раз

2. Практические результаты и ограничения

Опыт ранних внедрений свидетельствует о значительном повышении эффективности: агентства Министерства внутренней безопасности США после внедрения ИИ-систем обнаружения угроз зафиксировали сокращение числа успешных фишинговых атак на 47% в течение первого года эксплуатации. Эстония, признанный мировой лидер в области электронного государственного управления, использует алгоритмы машинного обучения для мониторинга государственных сетей в круглосуточном режиме, что позволило сократить среднее время реагирования на инциденты с нескольких часов до десяти минут. В Республике Узбекистан в рамках реализации стратегии «Цифровой Узбекистан — 2030» ведётся планомерное внедрение систем ИИ-мониторинга в инфраструктуру государственных порталов, хотя масштабирование этих решений по-прежнему остаётся актуальной задачей.

Вместе с тем применение ИИ сопряжено с рядом существенных ограничений. Модели машинного обучения подвержены состязательным атакам (adversarial attacks), при которых злоумышленник намеренно формирует входные данные,

вводящие систему в заблуждение. Проблема объяснимости алгоритмов («чёрный ящик») затрудняет юридическую верификацию принятых решений в государственном контексте, где подотчётность является базовым требованием. Наконец, дефицит квалифицированных специалистов по ИИ в государственном секторе и высокая стоимость инфраструктуры замедляют темпы внедрения, особенно в странах с формирующимися рынками.

3. Этические и правовые аспекты

Использование ИИ для мониторинга государственных информационных систем неизбежно поднимает вопросы баланса между безопасностью и правами граждан. Сбор и анализ поведенческих данных сотрудников требует чёткой правовой регламентации, прозрачных процедур получения согласия и ограничений по срокам хранения информации. Международный опыт показывает, что наиболее эффективными оказываются модели, сочетающие автономность ИИ в рутинных операциях с обязательным участием человека в принятии значимых решений — принцип «Human-in-the-Loop». Регуляторные рамки, подобные Акту ЕС об искусственном интеллекте (2024), классифицирующему системы биометрической идентификации как высокорисковые, задают вектор для разработки национального законодательства в данной сфере.

Заключение

Искусственный интеллект трансформирует информационную безопасность государственных органов, переводя её из области реактивного реагирования в плоскость предиктивной защиты. Практические результаты внедрения демонстрируют измеримое снижение числа успешных атак и времени реагирования на инциденты. Однако устойчивый эффект достигается лишь при комплексном подходе: сочетании технологических решений с развитием правовой базы, инвестициями в кадровый потенциал и соблюдением принципов этичного применения ИИ. Государственным органам Узбекистана и других стран с активно развивающейся цифровой инфраструктурой целесообразно сосредоточить усилия на создании межведомственных центров компетенций по ИИ-безопасности, поэтапном внедрении объяснимых моделей и гармонизации национального законодательства с передовыми международными стандартами.

СПИСОК ЛИТЕРАТУРЫ:

1. IBM Security. Cost of a Data Breach Report 2023. — Armonk: IBM Corporation, https://www.ibm.com/reports/data-breach

2. Европейский парламент. Регламент ЕС об искусственном интеллекте (AI Act). https://eur-lex.europa.eu/eli/reg/2024/1689/oj

3. Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials https://doi.org/10.1109/COMST.2015.2494502

4. Стратегия «Цифровой Узбекистан — 2030»: Указ Президента Республики Узбекистан https://lex.uz/docs/5031048

5. Goodfellow I., Bengio Y., Courville A. Deep Learning. — Cambridge: MIT Press, https://www.deeplearningbook.org/