THE ROLE OF INNOVATIVE TECHNOLOGIES IN THE PROTECTION OF CATEGORISED OBJECTS

Yakubov Jur'at Amangeldiyevich
Ministry of Defense of the public of Uzbekistan

Annotation. *This article analyses the theoretical and practical aspects of using innovative technologies to protect classified sites that require a high level of security, such as military facilities, strategic infrastructure, energy and transport systems. The possibilities, advantages and limitations of video analytics systems based on artificial intelligence, remote monitoring using Internet of Things (IoT) devices, and biometric identification systems are considered. Based on scientific sources, the study substantiates the effectiveness of real-time threat detection systems, anomaly detection, automated access control, and integrated security systems. It also proposes an architecture for creating a "smart security model" through the comprehensive integration of AI, IoT, and biometric systems, and highlights the measures necessary for such an approach in terms of cybersecurity, data privacy, and technical stability. Based on a systematic approach, the article reveals the role of modern digital security tools in protecting classified facilities.*

Key words: *categorised objects, artificial intelligence, video analytics, biometric systems, IoT (Internet of Things), remote monitoring, cybersecurity, edge computing, access control, anomaly detection, digital security, smart technologies.*

РОЛЬ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ В ОХРАНЕ КЛАССИФИЦИРОВАННЫХ ОБЪЕКТОВ

Якубов Журъат Амангелдиевич
Министерства обороны Республики Узбекистан

Аннотация. *В данной статье анализируются теоретические и практические аспекты использования инновационных технологий в охране категорированных объектов территорий, требующих высокой степени защиты, таких как военные объекты, стратегическая инфраструктура, энергетические и транспортные системы. Рассмотрены возможности, преимущества и ограничения систем видеоаналитики на основе искусственного интеллекта, дистанционного мониторинга с использованием устройств Интернета вещей (IoT), а также систем биометрической идентификации. В исследовании на основе научных источников обосновывается эффективность систем обнаружения угроз в режиме реального времени, регистрации аномальных ситуаций, автоматизации контроля доступа и интегрированных систем безопасности. Также предлагается архитектура создания "умной модели безопасности" путем комплексной интеграции ИИ, IoT и биометрических систем, а также освещаются меры, необходимые для такого подхода с точки зрения кибербезопасности, конфиденциальности данных и технической устойчивости.*

Статья на основе системного подхода раскрывает роль современных средств цифровой безопасности в защите категорированных объектов.

Ключевые слова: *категорированные объекты, искусственный интеллект, видеоаналитика, биометрические системы, IoT (Интернет вещей), дистанционный мониторинг, кибербезопасность, edge computing, контроль доступа, обнаружение аномальных ситуаций, цифровая безопасность, интеллектуальные технологии.*

TOIFALANGAN OBYEKTLARNI QO‘RIQLASHDA INNOVATSION TEXNOLOGIYALARNING ROLI

Yakubov Jur’at Amangeldiyevich
O‘zbekiston Respublikasi Mudofaa vazirligi

Annotatsiya. *Mazkur maqolada toifalangan obyektlarni harbiy obyektlar, strategik infratuzilma, energetika va transport tizimlari kabi yuqori darajada himoyalanishi zarur bo‘lgan hududlarni qo‘riqlashda innovatsion texnologiyalardan foydalanishning nazariy va amaliy jihatlari tahlil qilingan. Sun’iy intellektga asoslangan videoanalitika, Narsalar interneti (IoT) qurilmalari yordamida masofadan monitoring, shuningdek biometrik identifikatsiya tizimlarining imkoniyatlari, ustunliklari va cheklovlari ko‘rib chiqilgan. Tadqiqotda real-vaqt rejimida tahdidlarni aniqlash, anomal holatlarni qayd etish, kirish-chiqishni avtomatlashtirish va integratsiyalashgan xavfsizlik tizimlarining samaradorligi ilmiy manbalar asosida asoslab beriladi. Shuningdek, SI, IoT va biometrik tizimlarning kompleks integratsiyasi orqali “aqlli xavfsizlik modeli”ni yaratishning arxitekturasi taklif qilinadi va bunday yondashuvning kiberxavfsizlik, ma’lumotlar maxfiyligi hamda texnik barqarorlik nuqtai nazaridan talab qiladigan choralari yoritiladi. Maqola zamonaviy raqamli xavfsizlik vositalarining toifalangan obyektlarni himoya qilishdagi rolini tizimli yondashuv asosida ochib beradi.*

Kalit so‘zlar: *toifalangan obyektlar, sun’iy intellekt, videoanalitika, biometrik tizimlar, IoT (Narsalar interneti), masofadan monitoring, kiberxavfsizlik, edge computing, kirish nazorati, anomal holatlarni aniqlash, raqamli xavfsizlik, aqlli texnologiyalar.*

В условиях современной глобализации и резко меняющейся геополитической ситуации постоянно растущие требования безопасности вызывают необходимость обеспечения высокого уровня охраны категорированных объектов - военных объектов, стратегически важных инфраструктур, энергетических комплексов, транспортных коммуникаций и других объектов государственного значения. Поскольку традиционные методы охраны не обеспечивают достаточной эффективности на фоне сложности, оперативности и диверсификации современных угроз, резко возросла потребность в применении передовых цифровых технологий. В частности, интеграция искусственного интеллекта (ИИ), видеоаналитики, устройств IoT и систем биометрической аутентификации в сферу безопасности приводит к появлению совершенно новых подходов к защите объектов. Ускорение процесса цифровой

трансформации позволяет с помощью ИИ в режиме реального времени выявлять поведение, прогнозировать угрозы, автоматически фиксировать подозрительную деятельность [1; 2]. Устройства Интернета вещей расширяют функциональные возможности охраны, обеспечивая непрерывный удаленный сбор данных вокруг объекта, мониторинг через датчики, быструю интеграцию и обмен информацией между системами безопасности [3; 4]. При этом применение биометрических систем отпечатков пальцев, распознавания лица, радужной оболочки глаза, голоса и мультимодальной аутентификации существенно повышает точность и надежность контроля доступа [5; 6; 7].

Современные научные исследования отмечают возможность создания «умной модели безопасности» через комплексное применение этих технологий, при этом отмечается, что краевые вычисления, облачные вычисления, видеоаналитика, компьютерное зрение и обработка данных IoT в реальном времени создают новые стандарты безопасности [2; 3; 5]. В то же время вопросы, связанные с широким внедрением технологий, угрозы кибербезопасности, конфиденциальность данных, предотвращение подделки устройств с помощью PUF-технологий (Physical Unclonable Function), защита биометрических данных и обеспечение бесперебойной работы систем по-прежнему остаются актуальными [7; 8; 9].

Основная цель статьи состоит в анализе на основе научных источников возможностей, преимуществ и ограничений технологий искусственного интеллекта (ИИ), IoT и биометрических технологий в охране объектов, охраняемых по категориям, а также в предложении концепции интегрированной системы безопасности. В исследовании освещается роль этих технологий в мониторинге в реальном времени, контроле входа и выхода с высокой точностью, автономном выявлении опасного поведения и повышении эффективности комплексных охранных систем.

Искусственный интеллект и системы видеоаналитики.

1.1 Видеоаналитика + ИИ: основные возможности: в традиционных системах видеонаблюдения записывается только видео и наблюдение осуществляется через оператора-человека. Однако с помощью анализа видеоконтента на основе ИИ (video analytics / video intelligence) можно в реальном времени обнаруживать объекты, фиксировать движения или отклонения от нормы (например, несанкционированное лицо на территории, неизвестные движения, температура тела, нежелательное размещение) автоматически;

С помощью алгоритмов ИИ идентифицируются люди, транспортные средства, объекты, их движение и поведение — это позволяет раннее обнаружение преступной деятельности, беспричинного доступа, нежелательных движений;

Кроме того, edge computing + ИИ тоже важны: около камер (на краевых устройствах) анализ видео позволяет уменьшить объем передаваемых по сети данных, сократить задержку (latency) и обеспечить мониторинг в реальном времени.

1.2 Примеры / Эмпирические исследования: например, в статье A Smart, Efficient, and Reliable Parking Surveillance System with Edge Artificial Intelligence on IoT Devices мониторинг парковок осуществлялся с использованием edge-AI + IoT камер; в реальных условиях обнаружено более 95% точности.

В другом научном анализе рассматривается выявление преступлений и актов агрессии с помощью видеонаблюдения и машинного обучения в условиях умного города в 2018-2024 годах.

1.3 Ограничения и риски: системы видеонаблюдения и ИИ работают с большими объемами данных, что может создать значительную нагрузку на сети и инфраструктуру хранения. Edge computing и оптимизированные алгоритмы частично решают эту проблему;

однако, если система настроена неправильно, возможны ошибочные определения, случаи ложноположительных / ложноотрицательных результатов (то есть ложные предупреждения или игнорирование реальных угроз), что ослабляет безопасность предприятия или военного объекта. Этот вопрос требует серьезного и тщательного рассмотрения.

Устройства IoT (Internet of Things - Интернет вещей) и дистанционный мониторинг.

2.1 IoT + видеонаблюдение: архитектура и преимущества: Статья "IoT video analytics for surveillance-based systems in smart cities" показывает, что сеть датчиков и камер IoT в сочетании с машинным обучением обеспечивает анализ видеопотоков в режиме реального времени, обнаружение поведения и оповещение;

"Умные" сигналы и датчики на базе IoT - такие как обнаружение движения, температуры, освещенности, уровня воды/газа, пожара, объектов за стеной - этот тип комплексного мониторинга позволяет выявлять различные угрозы на ранней стадии;

дистанционный мониторинг: IoT + облачная или серверная архитектура (cloud-assisted) - например, пользователи IoT-камер, сенсорных устройств и интерфейсов удаленного доступа могут отслеживать ситуацию в режиме реального времени из любой точки.

2.2 Сети IoT и аспекты кибербезопасности: однако по мере расширения сетей IoT возрастают и риски кибербезопасности: могут возникнуть такие проблемы, как уязвимости устройств и их подключения к сети, несанкционированный доступ, искажение данных, кража видео и информации;

например, в статье "Secure biometric-based access control scheme for future IoT-enabled cloud-assisted video surveillance system" представлена схема биометрической аутентификации и взаимной аутентификации через облачный сервер, а также шифрования данных с помощью сессионных ключей для систем видеонаблюдения IoT. Этот подход служит для усиления безопасности IoT и биометрической защиты.

2.3 Архитектура применимого проекта для объектов, отнесённых к данной категории.

В вашем случае для объектов данной категории предпочтительна следующая концептуальная архитектура:

Edge/IOT-камеры + умные сенсоры (движение, объекты за стеной, доступ в ограниченную зону, изменение огня/газа/воздуха);

Анализ видеопотоков на краю (в реальном времени), сигнал на сервер/центральную службу мониторинга только в случае аномалии или угрозы;

Облачный/локальный сервер + ИИ-видеаналитика + архив видео / база данных состояний;

Дистанционный мониторинг и управление — операторы, ответственные сотрудники через умные устройства, компьютеры следят за состоянием системы, контролируют входы/выходы.

3. **Биометрические системы и их эффективность в обеспечении безопасности.**

3.1 Преимущества биометрической идентификации и аутентификации: биометрические системы (распознавание лица, радужной оболочки глаза, отпечатков пальцев, биометрических поведенческих характеристик) позволяют доступ осуществлять только авторизованным лицам. Это существенно повышает безопасность по сравнению с такими методами, как традиционный ключ, карта, пароль, потому что биометрические данные уникальны и привязаны к личности;

через интеграцию биометрии + IoT + видеонаблюдения — например, распознавание лиц + видеаналитика + система контроля доступа — можно создать «системную безопасность», то есть объединённый контроль доступа, перемещений и наблюдения. Подобные комплексные системы подходят для объектов, требующих повышенного уровня надёжности.

3.2 Примеры следующих научных исследований: статья «Secure biometric-based access control scheme ...», упомянутая выше, рекомендует интеграцию биометрической аутентификации и видеонаблюдения на базе IoT и управление доступом к видеопотокам в реальном времени через облако; показано, что этот метод безопасен против пассивных и активных атак;

Кроме того, в статье IoT based Biometric Access Control System описана система контроля доступа по отпечаткам пальцев через биометрическую систему и IoT-сеть, а также интеграция онлайн-баз данных.

3.3 Безопасность и ограничения, меры предосторожности:

биометрические данные (лицо, отпечатки пальцев, радужная оболочка глаза и т. п.) должны быть надлежащим образом защищены; если данные хранятся на общедоступных серверах, или в сетях IoT без шифрования — данные могут быть украдены, скопированы, неправомерно использованы;

Также необходимо применение технических подходов, таких как защита биометрических шаблонов (например, отменяемые биометрические данные + биокриптография). Например, в исследовании под названием Hybrid Template

Protection Scheme for Face Recognition in IoT-based Environments рассмотрены способы обеспечения безопасности биометрических шаблонов — такие методы, как FaceHashing и S-XOR. Кроме того, биометрические системы подвержены угрозе поддельных биометрических образцов (spoofing) — через фотографию, видео, маску, 3D-маску. По этой причине следует применять проверку живости (liveness detection), двухфакторную аутентификацию и другие меры защиты.

4. Интегрированная модель: Искусственный интеллект + IoT + Биометрические системы.

4.1 Концепция комплексной системы и ее преимущества: для категорированных объектов - особенно объектов военного, энергетического, транспортного, стратегического предприятия - может быть недостаточно только одного слоя защиты. Поэтому:

Video surveillans + SI video-analytics (определение угроз в реальном времени);

IoT сенсорная/камерная сеть + дистанционный мониторинг и автоматическая сигнализация;

Биометрический контроль доступа + аутентификация + достаточная защита шаблонов;

Эта архитектура создает резерв: если один ломается - другие обеспечивают безопасность. Кроме того, интеграция ИИ + IoT + биометрия увеличивает доступ к объекту, действия внутри, раннее обнаружение состояния посторонних лиц и опасных действий, а также возможность реагирования в режиме реального времени.

4.2 Практические рекомендации и аспекты реализации:

При выборе устройств Edge-IoT и видеоаналитики данные следует анализировать локально, без отправки в сеть (для пропускной способности и конфиденциальности);

Необходимо шифрование биометрических данных, защиту шаблонов (cancelable biometrics, биокриптография), постоянное обновление и внедрение детекции живости;

Политика кибербезопасности, защита сетей, хранение и передача данных, стандарты (шифрование, аутентификация, ведение журналов) должны быть разработаны — особенно в IoT-системах.

Интеграция искусственного интеллекта (ИИ), Интернета вещей (IoT) и биометрических систем представляет собой эффективный и современный подход к защите объектов с ограниченным доступом и критической инфраструктуры. Эти технологии существенно повышают уровень безопасности благодаря взаимодополняющим функциям, обеспечивают мониторинг в реальном времени и позволяют выявлять угрозы на ранней стадии. Алгоритмы ИИ помогают обнаруживать нестандартные действия, несанкционированное проникновение и агрессивное поведение через видео-наблюдение, а в сочетании с edge computing снижают объем данных, передаваемых в сеть, и минимизируют задержки. Устройства IoT с

расширенными сенсорными сетями постоянно контролируют температуру, уровень пожара, газа, движение и другие параметры, что обеспечивает оператору возможность получать сигналы в реальном времени и своевременно выявлять угрозы. Биометрические системы ограничивают доступ только авторизованным лицам, значительно повышая безопасность по сравнению с традиционными системами ключей, карт или паролей. Таким образом, интеграция этих трех технологий создает избыточность: при сбое одной системы другие продолжают обеспечивать безопасность и повышают общую устойчивость системы. Однако для IoT-сетей и биометрических данных критически важны меры кибербезопасности, включая шифрование, защиту шаблонов и технологии против подделки (spoofing). Поэтому оптимальная стратегия для объектов с ограниченным доступом заключается в подходе «многоуровневая защита, технологическая интеграция и кибер/защитные меры», обеспечивающем оперативный отклик, выявление угроз и поддержание стабильности системы.

СПИСОК ИСПОЛЬЗОВАННЫХ ЛИТЕРАТУР:

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). *Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications.* IEEE Communications Surveys & Tutorials, **17**(4), 2347–2376. course.ccs.neu.edu+2Elmi+2

2. Satyasree, K. P. N. V., Gongada, T. N., Upadhayaya, N., Naresh, E., Patra, J. P., & Kaur, M. (2023). *Edge AI for Real-Time Video Analytics in Surveillance Systems.* International Journal on Recent and Innovation Trends in Computing and Communication, **11**(10), 2269–2275. ijritcc.org

3. *Edge-Computing-Enabled Abnormal Activity Recognition for Visual Surveillance.* Electronics, **13**(2), 251. (2024). MDPI

4. Zhang, R., & Yan, Z. (2019). *A Survey on Biometric Authentication.* IEEE Access, **7**, 5994–6009. Aalto Doc+1

5. Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C. (2021). *Biometrics for Internet-of-Things Security: A Review.* Sensors, **21**(18), 6163. MDPI+1

6. Sundararajan, A., Sarwat, A. I., & Pons, A. (2019). *A Survey on Modality Characteristics, Performance Evaluation Metrics, and Security for Traditional and Wearable Biometric Systems.* arXiv preprint. arXiv

7. Shamsoshoara, A., Korenda, A., Afghah, F., & Zeadally, S. (2019). *A Survey on Physical Unclonable Function (PUF)-based Security Solutions for Internet of Things.* arXiv preprint. arXiv

8. *A Survey of Protocols and Standards for Internet of Things.* arXiv preprint (Salman, T., & Jain, R.). (2020). arXiv

9. Qadir, Q. M., Rashid, T. A., Al-Salihi, N. K., Ismael, B., Kist, A. A., & Zhang, Z. (2020). *Low Power Wide Area Networks: A Survey of Enabling Technologies, Applications and Interoperability Needs.* arXiv preprint. arXiv

10. *Comprehensive survey: Biometric user authentication application, evaluation, and discussion.* Computers and Electrical Engineering, **119**, 109485. (2024). ScienceDirect