DOI: 10.12731/2227-930X-2024-14-2-292
УДК 621.397.42

Научная статья | Системный анализ, управление и обработка информации

АНАЛИЗ БЕЗОПАСНОСТИ ГОРОДСКИХ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ: УЯЗВИМОСТИ И СТРАТЕГИИ ЗАЩИТЫ

А. Исрафилов, П.Р. Ситников, А.Д. Соколов, А.Ю. Ишанхонов, И.Ю. Благова

В эпоху цифровизации городских пространств, системы видеонаблюдения играют ключевую роль в обеспечении общественной безопасности. Однако уязвимости в программном обеспечении и аппаратной части этих систем могут привести к серьезным нарушениям приватности и безопасности. Важность этой темы обусловлена растущим количеством кибератак и утечек данных, целями которых часто становятся городские инфраструктуры.

Цель. *Целью данной статьи является анализ уязвимостей систем видеонаблюдения в контексте городской инфраструктуры, а также определение потенциальных рисков для безопасности данных и личной приватности. Статья стремится выявить слабые места в технологиях и предложить рекомендации по их устранению.*

Методы исследования. *Для анализа использовались методы анализа данных о нарушениях в системах видеонаблюдения за последние пять лет и обзор современных технологий: Изучение современных методов шифрования и практик регулярного обновления программного обеспечения, направленных на минимизацию рисков.*

Результаты. *Исследование показало, что большинство систем видеонаблюдения уязвимы к атакам среднего уровня сложности. Наиболее часто встречающиеся уязвимости связаны с недостаточным шифрованием данных и устаревшим программным обеспечением. В результате анализа были разработаны предложения по усилению защиты данных, включая регулярное обновление ПО, использование многоуровневых систем аутентификации и шифрования.*

Область применения результатов. *Полученные результаты и рекомендации по укреплению систем видеонаблюдения могут быть применены в различных сферах городской инфраструктуры, включая общественный транспорт, муниципальные учреждения и коммерческие объекты. Особенно актуально применение этих рекомендаций для объектов с высокой проходимостью людей и повышенными требованиями к безопасности, таких как школы, больницы и торговые центры. Эффективное внедрение предложенных технологий шифрования и усиленные меры безопасности помогут предотвратить не только утечки данных, но и потенциальные акты терроризма или другие угрозы безопасности граждан.*

Ключевые слова: *городская инфраструктура; видеонаблюдение; камеры видеонаблюдения; системы видеонаблюдения; шифрование данных; кибербезопасность; обновление программного обеспечения; защита приватности; хранение данных; кибератаки*

Для цитирования. *Исрафилов А., Ситников П.Р., Соколов А.Д., Ишанхонов А.Ю., Благова И.Ю. Анализ безопасности городских систем видеонаблюдения: уязвимости и стратегии защиты // International Journal of Advanced Studies. 2024. Т. 14, № 2. С. 7-31. DOI: 10.12731/2227-930X-2024-14-2-292*

Original article | System Analysis, Management and Information Processing

SECURITY ANALYSIS OF URBAN VIDEO SURVEILLANCE SYSTEMS: VULNERABILITIES AND PROTECTION STRATEGIES

A. Israfilov, P.R. Sitnikov, A.D. Sokolov, A.Yu. Ishankhonov, I.Yu. Blagova

In the era of digitalization of urban spaces, video surveillance systems play a key role in ensuring public safety. However, vulnerabilities in the software and hardware of these systems can lead to serious pri-

vacy and security breaches. The importance of this topic is due to the growing number of cyber attacks and data leaks, the targets of which are often urban infrastructure.

Purpose. *The main aim of this article is to analyze the vulnerabilities of video surveillance systems in the context of urban infrastructure, as well as to identify potential risks to data security and personal privacy. The article seeks to identify weaknesses in technologies and offer recommendations for eliminating them.*

Methodology. *The analysis used methods for analyzing data on violations in video surveillance systems over the past five years and a review of modern technologies: Study of modern encryption methods and practices of regular software updates aimed at minimizing risks.*

Results. *The study showed that most video surveillance systems are vulnerable to medium-level attacks. The most common vulnerabilities are related to insufficient data encryption and outdated software. As a result of the analysis, proposals were developed to strengthen data protection, including regular software updates and the use of multi-level authentication and encryption systems.*

Practical implications. *The findings and recommendations for strengthening surveillance systems can be applied across various sectors of urban infrastructure, including public transportation, municipal institutions, and commercial facilities. The implementation of these recommendations is particularly critical for locations with high foot traffic and elevated security requirements, such as schools, hospitals, and shopping centers. Effective adoption of the proposed encryption technologies and enhanced security measures will help prevent not only data breaches but also potential acts of terrorism or other security threats to citizens.*

Keywords: *urban infrastructure; video surveillance; surveillance cameras; video surveillance systems; data encryption; cybersecurity; software updating; privacy protection; data storage; cyberattacks*

For citation. *Israfilov A., Sitnikov P.R., Sokolov A.D., Ishankhonov A.Yu., Blagova I.Yu. Security Analysis of Urban Video Surveil-*

lance Systems: Vulnerabilities and Protection Strategies. International Journal of Advanced Studies, 2024, vol. 14, no. 2, pp. 7-31. DOI: 10.12731/2227-930X-2024-14-2-292

Введение

В условиях увеличения плотности населения в крупных городах вопросы безопасности приобретают особую значимость. Камеры видеонаблюдения (КВ), выполняющие функции контроля за обстановкой в общественных пространствах, транспортных узлах и других стратегически важных объектах, играют ключевую роль в поддержании общественного порядка. Несмотря на значительные преимущества, данные технологии имеют некоторые недостатки, которые могут быть использованы для получения конфиденциальной информации и кибератак.

Основная часть

КВ предназначены для визуального мониторинга территорий, объектов и людей. Они позволяют фиксировать, хранить и анализировать изображения с целью обеспечения безопасности, контроля и оперативного реагирования на чрезвычайные ситуации.

Видеонаблюдение впервые применили в 1942 году для мониторинга запуска ракет в Германии во время Второй мировой войны. Однако широкое распространение технологии началось в 1970-х годах благодаря развитию способов записи и передачи видео.

На текущий, 2024 год, объем мирового рынка СВН оценивается в 81,68 млрд. долларов. По прогнозу рынок достигнет 145,38 млрд. долларов к 2029 году, увеличившись в среднем на 12,22% в течение прогнозируемого периода [1]. Значительный рост использования СВН в последнее время фиксируется в Азиатско-Тихоокеанском регионе, особенно в Китае, где правительство финансирует установку СВН в общественных местах для повышения уровня безопасности. В 2023 году Китай стал лидером по количеству КВ на 1000 человек с показателем 439,07 (рис.1).

Рис. 1. Количество КВ в городах мира на 1000 чел, шт [2]

СВН являются частью стратегий устойчивого развития, направленных на повышение качества жизни граждан, обеспечение эффективного городского управления и безопасности на национальном и глобальном уровнях.

Отметим, что в крупных российских городах, таких как Москва и Санкт-Петербург, количество КВ на 1000 человек выше, чем в среднем в Европе или в США. Это свидетельствует о повышенном внимании к вопросам общественной безопасности и стремлении к обеспечению контроля в условиях городской среды. Усиленное использование СВН помогает в профилактике преступлений и повышении уровня защищенности граждан. По оценкам аналитиков, в период до 2028 года объем российского рынка видеонаблюдения будет расти на 10-12% в год и достигнет 24 млрд. рублей [3]. СВН преимущественно используются государственными структурами: проекты «Безопасный город», «Антитеррор», системы безопасности метро, аэропортов и вокзалов.

Классификация КВ

Для обеспечения эффективного видеонаблюдения в городской инфраструктуре [4] используются различные типы КВ, каждый из которых предназначен для конкретных задач и условий эксплуатации:

1) Купольные КВ получили свое название благодаря наличию полусферического кожуха. Он не только защищает камеру от внешних воздействий, но и делает направление объектива менее заметным. У устройств широкий угол обзора, поэтому они часто применяются в общественных местах.

2) Камеры-пули имеют цилиндрическую форму. Используются для мониторинга больших открытых пространств.

3) КВ коробчатого типа – традиционный тип камер, которые обладают большим набором настроек объектива. Это позволяет использовать их для наблюдения на значительных расстояниях или в особых условиях освещенности.

4) PTZ-камеры (pan-tilt-zoom) могут поворачиваться горизонтально и вертикально, а также изменять фокусное расстояние. Применяются в городских наблюдательных системах, больших торговых залах или для обеспечения безопасности на массовых мероприятиях.

5) КВ с объективом Fisheye обеспечивают сверхширокий угол обзора. Используются на больших открытых пространствах.

6) Мультисенсорные КВ сочетают несколько объективов и датчиков в одном устройстве, обеспечивая мультидирекциональный обзор и возможность мониторинга нескольких направлений одновременно без слепых зон. Они часто применяются в сложных системах безопасности.

7) КВ клинового типа обладают компактным дизайном, что важно для дискретного мониторинга. Используются в условиях, требующих минимального внимания к установленной системе видеонаблюдения, таких как магазины, частные дома или офисы.

Статистика показывает, что КВ купольного типа являются самыми популярными на рынке из-за их широкого угла обзора (рис.2).

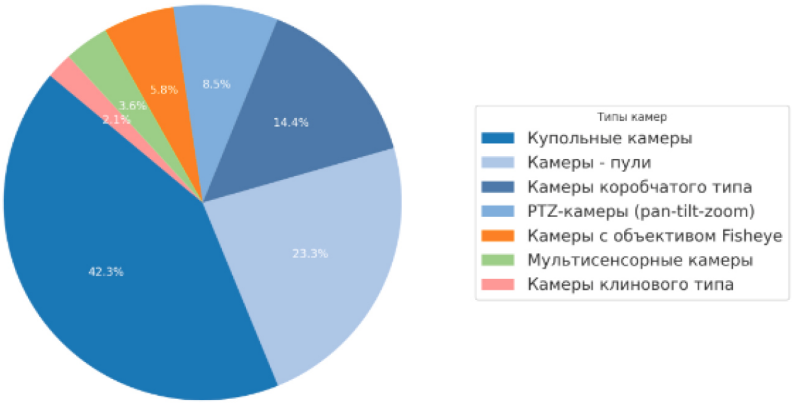

Рис. 2. Популярность использования разных типов КВ в городской среде [5]

По типу сигнала наиболее распространенными являются аналоговые и цифровые СВН:

1) Аналоговые СВН используют телевизионное вещание для передачи видео по коаксиальному кабелю. Они просты в эксплуатации и имеют низкую стоимость установки и обслуживания, поэтому чаще всего используются в небольших торговых точках или на предприятиях.

2) Цифровые СВН передают данные через IP-сети. Это позволяет применять современные методы обработки изображений, такие как распознавание лиц и анализ поведения.

В последние годы наблюдается снижение доли аналоговых СВН на фоне увеличения сегмента IP-камер и СВН с интеграцией искусственного интеллекта (ИИ) [6]. Объем мирового рынка IP-камер достиг 12,2 млрд. долларов в 2023 году. Прогнозируется, что показатель вырастет до 33,4 млрд. долларов к 2032 году со среднегодовыми темпами роста в 11,83% [7]. Это обусловлено необходимостью получения изображений более высокого качества для предупреждения и предотвращения незаконного поведения людей, например, нарушения правил дорожного движения.

Лидером по количеству дорожных КВ является Россия – 18 424 штуки [8]. Второе место занимает Бразилия (17 939 КВ), третье – Италия (11 296 КВ), четвертое – США (8 129 КВ). Это свидетельствует о высокой приоритетности вопросов безопасности дорожного движения в этих странах и стремлении правительств использовать технологические решения для контроля и управления транспортными потоками, а также для повышения общей безопасности.

Среди СВН стоит выделить технологии, интегрированные с другими элементами безопасности, например, с системами контроля доступа. Это позволяет усилить защиту объекта на основе верификации личности и предотвратить несанкционированный доступ [9].

Внедрение в городские КВ программного обеспечения (ПО) для анализа видео позволяет автоматизировать процесс мониторинга и увеличивает его эффективность. Технологии распознают аномалии в поведении людей и предупреждают о возможных угрозах в реальном времени. Это способствует созданию более безопасных пространств. Например, в Лондоне КВ подключены к системе экстренного реагирования, что позволяет полиции оперативно прибывать на место происшествия.

Основные уязвимости КВ

Сбои в работе КВ представляют серьезную угрозу для общественной безопасности. Они могут быть вызваны системными или программными уязвимостями.

Системные уязвимости представляют собой дефекты в аппаратном обеспечении КВ. Они включают недостаточную защиту устройств от физических воздействий и вмешательств, что может привести к несанкционированному доступу к камерам [10].

В ответ потенциальные вызовы компания Axis Communications (Швеция) выпустила серию уличных КВ с улучшенной устойчивостью к вандализму. Устройства оснащены усиленными корпусами и специальными защитными козырьками, что повышает их стойкость к механическим повреждениям.

Компания Honeywell (США) выпускает КВ с интегрированным датчиком движения. В случае попытки физического воздействия на устройство, система автоматически активирует звуковую и световую сигнализацию, что привлекает внимание к инциденту и ускоряет реакцию служб безопасности. Эти примеры показывают, как улучшение конструктивных характеристик аппаратного обеспечения КВ может снизить риски, связанные с системными уязвимостями.

В России, в ответ на уязвимости СВН связанные с физическими воздействиями, были разработаны камеры с улучшенной противоударной защитой. Например, компания «Ростелеком» интегрировала в КВ специальные антивандальные корпуса, которые устойчивы к попыткам взлома. Это значительно повышает безопасность установленных устройств и снижает риск несанкционированного доступа к данным, обеспечивая надежную защиту как для частных, так и для государственных объектов.

Программные уязвимости связаны с ошибками во встроенном ПО КВ. Они могут быть использованы злоумышленниками для контроля над устройством или получения доступа к передаваемым данным [11].

В 2021-2023 гг. более полумиллиона IP-камер китайской компании Hikvision были взломаны за счет уязвимости CVE-2021-36260 [12]. Киберпреступники отправляли на веб-серверы СВН специальные сообщения, которые позволяли в дальнейшем получать контроль над устройствами. Уязвимость возникла вследствие отсутствия систематических обновлений систем и слабых паролей на устройствах.

В 2022 году в СВН ZoneMinder была обнаружена уязвимость, позволяющая злоумышленникам подключаться к внутренней сети клиентов и получать доступ к видеопотоку [13]. На тот период большее количество пользователей ZoneMinder проживало в США (17 % от общего количества). В Польше – 15 %, в Италии – 11 %, в Германии и Люксембурге по 7 %, в России – 6 %. Все они оказались под угрозой кибератаки с целью получения сведений.

В этот же период российская компания «Информзащита» успешно обновила ПО КВ после обнаружения уязвимости, которая позволяла злоумышленникам получить несанкционированный доступ к данным. Благодаря быстрому реагированию и внедрению патчей, были предотвращены возможные кибератаки и обеспечен высокий уровень защиты персональных данных пользователей и общественной безопасности [14].В общей сложности в 2023 году в России отразили более 65 000 кибератак на объекты критической инфраструктуры. Это подчеркивает высокий уровень развития СВН и защиты данных в стране, подтверждая эффективность внедренных мер безопасности. Российские технологии видеонаблюдения, оснащенные передовыми алгоритмами обнаружения угроз и автоматической реакцией на инциденты, демонстрируют способность не только к активному отслеживанию, но и к оперативному предотвращению потенциальных взломов.

Тем не менее, наличие уязвимостей в СВН во всем мире подчеркивает необходимость постоянного обновления систем безопасности, использования современных методов криптографической защиты и реализации многоуровневых систем аутентификации для управления доступом к городским КВ.

Риски и последствия эксплуатации уязвимостей КВ

Использование злоумышленниками системных и программных уязвимостей может привести к серьезным последствиям, например, к **нарушению неприкосновенности частной жизни** [15]. Разглашение личной информации граждан путем незаконного распространения данных с КВ противоречит нормам Общего регламента по защите данных (GDPR) в Европейском Союзе, Конвенции о защите прав человека и основных свобод, Международного пакта о гражданских и политических правах, Закона Калифорнии о конфиденциальности потребителей (CCPA), ФЗ «О персональных данных» РФ и многих других национальных и международных официальных документов.

КВ часто собирают информацию без явного согласия наблюдаемых лиц, что ставит под угрозу право людей на конфиденциальность. Внедрение технологий распознавания лиц в системы городского видеонаблюдения приводит к созданию баз данных личных изображений, доступ к которым может быть получен не только государственными органами, но и злоумышленниками в случае несанкционированного обнародования.

Так, в Вашингтоне (США) злоумышленники взломали СВН полицейского управления с помощью уязвимости в программном обеспечении [16]. Они получили доступ к камерам, расположенным в различных частях города. Это позволило мошенникам наблюдать за действиями граждан в реальном времени, а также просматривать записи, содержащие персональные данные.

В 2021 году хакеры получили доступ к 150 000 камер компании Verkada (США) по всему миру. Устройства были установлены на различных объектах, включая больницы, школы, компании (Tesla Inc), отделения полиции и тюрьмы [17]. Злоумышленники получили возможность просматривать как живые трансляции, так и архивные записи видео, что позволило использовать личные данные. Инцидент привел к усиленному контролю за ИБ и стимулировал ужесточение требований к протоколам защиты частной жизни людей.

Проблема конфиденциальности информации усложняется, когда КВ интегрируются с другими технологиями, например, с системами «умного дома» или мобильными приложениями. По прогнозам, рынок КВ на частных территориях достигнет 30,10 млрд. долларов к 2030 году с совокупным годовым темпом роста в 19,2%. При этом количество домовладений, в которых установлены интеллектуальные камеры, в 2027 году составит 180,7 млн (рис. 3).

Исследователи из международной компании Checkmarx в 2022 году обнаружили уязвимость в камерах Ring от Amazon (США) [19]. Это распространенная модель, которая позволяет пользователям управлять устройствами в доме через мобильное

приложение. Из-за недостатков в системе ИБ появился риск незаконного распространения частных видеозаписей. Обновление ПО видеокамер помогло устранить проблему.

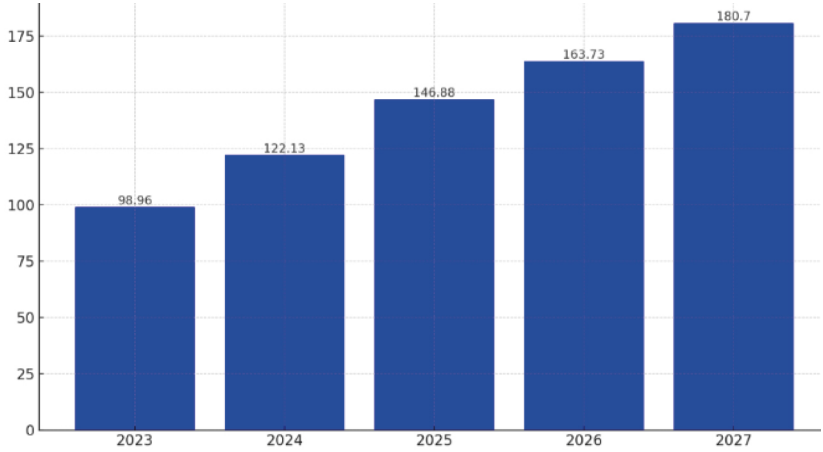

Рис. 3. Количество домовладений с интеллектуальными камерами безопасности во всем мире, млн. [18]

Несанкционированный доступ к КВ может быть осуществлен с целью **наблюдения за объектами критической инфраструктуры** и создания помех в их работе. В январе 2022 года в Вашингтоне хакеры нарушили функционирование СВН полицейского управления. Злоумышленники получили доступ к КВ, установленными в районах города для обеспечения безопасности, на 48 часов [20]. Последствия взлома оказались значительными: полиция потеряла доступ к онлайн-мониторингу происшествий и реагированию на них.

В России в 2023 году начали разрабатывать метод на основе ИИ, который помогает пресекать попытки обойти защиту СВН. Ранее злоумышленники могли внедряться в системы и искажать передаваемые данные таким образом, что посторонние объекты воспринимались КВ как часть фона. Внедрение новых технологий направлено на комплексную защиту СВН от подобных ин-

цидентов, что особенно важно для объектов критической инфраструктуры [21].

Уязвимости видеонаблюдения могут быть использованы для **проведения кибератак с целью дестабилизации экономической ситуации.** Атаки на КВ могут происходить за счет распространения вирусов, которые поражают сегменты сети и провоцируют сбои в работе камер. Это приводит к потере данных и значительным финансовым убыткам для предприятий и государственных структур из-за восстановления работы устройств.

Технические уязвимости СВН создают **риски внедрения вредоносного ПО.** Оно обеспечивает злоумышленникам возможность не только перехватывать потоки данных, но и управлять функционированием самих камер. Это может привести к несанкционированному изменению настроек устройств или их отключению в важный момент. В результате, возможности для мониторинга и реагирования на реальные угрозы значительно снижаются, создавая угрозы для безопасности городской инфраструктуры.

Использование уязвимостей в КВ несет за собой **риск создания аварийных ситуаций на транспорте и в общественных местах** [22]. Внешнее управление устройствами может привести к неправильной интерпретации событий службами безопасности и спровоцировать неправомерные действия, например, мобилизацию правоохранительных органов. КВ могут выступить инструментами манипуляции, что способствует дестабилизации общественного порядка и влияет на стратегические решения в чрезвычайных ситуациях. Например, взлом КВ в общественных местах может привести к эвакуации людей при отсутствии реальной угрозы безопасности.

Уязвимости КВ, особенно тех, которые используют технологии распознавания лиц, могут создавать серьезные **проблемы для правосудия,** включая риск привлечения к ответственности невиновных людей. Ошибки идентификации возникают по различным причинам, включая низкое качество изображения, изме-

нения во внешности человека, или системные сбои. Так, полиция Детройта (США) арестовала гражданина по подозрению в краже часов. Позже выяснилось, что он не имел к преступлению никакого отношения. Ошибка произошла по вине видеосистемы распознавания лиц, которая перепутала мужчину с настоящим преступником [23].

В России к системе распознавания лиц подключена каждая третья КВ. Лидером по внедрению СВН является Москва, где за последние 10 лет количество зарегистрированных преступлений на улицах уменьшилось в два раза, а количество угонов – в 10 раз [24]. В целом раскрываемость преступлений выросла вдвое, что подтверждает значительное усиление общественной безопасности благодаря эффективному использованию СВН с функциями распознавания лиц.

Методы оценки и минимизации рисков

В рамках обеспечения безопасности городской инфраструктуры особое внимание уделяется оценке рисков, связанных с уязвимостями КВ. Такие процедуры включают идентификацию потенциальных угроз, анализ слабых мест и разработку мер по их устранению. В таблице 1 представлена классификация методов, которые могут быть применены для совершенствования ИБ.

По мнению автора, изучение и применение данных методов позволяет не только оценить существующие и потенциальные риски, но и разработать эффективные стратегии для их минимизации. Основываясь на анализе, можно определить приоритетные направления для укрепления безопасности СВН, что способствует повышению общей устойчивости городских информационных систем к киберугрозам. Это подтверждается успешной практикой российской компании «Информзащита», которая внедрила продвинутые системы обнаружения вторжений и анализа аномалий в поведении сетевого трафика. Использование интегрированных решений, включая шифрование

данных и аутентификацию на основе биометрии, позволило значительно снизить вероятность несанкционированного доступа к СВН. Внедрение этих технологий в комплекс с регулярными обновлениями безопасности и обучением персонала на специализированных курсах, предоставляет компании возможность оперативно реагировать на угрозы, повышая таким образом надежность и доверие к используемым СВН.

Таблица 1.

Методы оценки и минимизации рисков атак на КВ

Метод оценки рисков	Инструменты контроля	Преимущества	Недостатки
Аудит	ПО для мониторинга изменений, утилиты для сканирования уязвимостей, такие как Nessus или Qualys, использование стандартов ISO/IEC 27001, аудиты Федеральной службы по техническому и экспортному контролю России	Детальный обзор безопасности систем.	Требует регулярного обновления программ и высокой квалификации персонала.
Тестирование на проникновение (моделирование атаки)	Автоматизированные инструменты тестирования. Применение фреймворков, например, Metasploit.	Имитирует реальные атаки для проверки устойчивости систем.	Может быть дорогостоящим и требует специализированных знаний [27].
Анализ потенциальных угроз	Использование ПО, например, RSA Archer.	Определяет наиболее вероятные угрозы.	Может не учитывать новые или нестандартные угрозы.
Комплексная оценка уязвимостей	Многоуровневая система защиты. Интеграция физических барьеров и сетевых межсетевых экранов (firewalls), систем обнаружения и предотвращения вторжений (IDS/IPS); российские системы защиты информации «Аккорд»	Обеспечивает защиту на нескольких уровнях.	Трудоемкий метод, может потребовать значительных вложений.

В контексте обеспечения ИБ городской инфраструктуры, важное значение имеет применение стратегий минимизации рисков, связанных с уязвимостями КВ. Одной из основных мер является регулярное обновление ПО и оборудования. Это не только предотвращает использование мошенниками известных уязвимостей, но и способствует интеграции актуальных достижений в области технологий защиты.

Еще одним направлением является шифрование данных. Оно обеспечивает безопасность передаваемой информации, делая ее бесполезной для злоумышленников. Использование современных стандартов шифрования, таких как AES и TLS, является обязательным условием для повышения устойчивости СВН к внешним угрозам.

Разработка правил и нормативов ИБ играет ключевую роль в минимизации рисков [25]. Стандарты помогают унифицировать обязательства по ИБ на всех этапах использования СВН от производства до эксплуатации. Они включают требования к регистрации операций с системой, к управлению доступом, аудиту активности и реагированию на инциденты. Например, международный стандарт ISO/IEC 27001 регламентирует рамки установления, реализации, поддержания и непрерывного улучшения системы управления ИБ [26]. Это обеспечивает систематический подход к защите конфиденциальности, целостности и доступности информационных активов, что особенно важно в контексте использования КВ в городской среде.

Эффективная реализация стратегий минимизации рисков способствует не только предотвращению непосредственных киберугроз, но и создает условия для устойчивого развития урбанистической среды, повышая уровень жизни граждан [27]. Компаниям необходимо поддерживать высокие стандарты в области ИБ и постоянно адаптироваться к новым вызовам и угрозам, чтобы защитить общественные и частные интересы в динамично меняющемся технологическом ландшафте.

Заключение

Обеспечение ИБ городской инфраструктуры через КВ требует комплексного подхода, включая постоянное обновление и модернизацию технологических средств. Необходима интеграция передовых методов шифрования и регулярное обновление ПО для защиты от новейших угроз. Внедрение строгих нормативов позволяет стандартизировать механизмы ИБ и повышать надежность СВН. Совершенствование методов защиты данных и управление доступом становятся ключевыми в борьбе с киберпреступностью, способствуя созданию безопасного и стабильного урбанистического пространства.

Подходы к городскому видеонаблюдению значительно отличаются в разных странах. В Европе и США особое внимание уделяется развитию законодательной базы, которая регулирует сбор и обработку персональных данных. Это сопровождается широким использованием облачных технологий и больших данных для анализа и управления городскими услугами, требующими внедрения продвинутых механизмов защиты. В России, где количество установленных камер видеонаблюдения одно из самых высоких в мире, ситуация выглядит более благоприятной. Это связано с эффективностью использования КВ в системах безопасности, а также с активным внедрением современных технологий шифрования и автоматизации обработки данных. Такой подход позволяет России успешно противостоять киберугрозам, обеспечивая высокий уровень защиты информации в городских СВН.

Список литературы

1. Video Surveillance Market Size & Share Analysis – Growth Trends & Forecasts (2024-2029). URL: https://www.mordorintelligence.com/industry-reports/video-surveillance-systems-market (дата обращения: 05.04.2024)
2. Surveillance camera statistics / Surveillance Studies. URL: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ (дата обращения: 02.04.2024)

3. ИАА TelecomDaily: рынок ВА может вырасти в два раза / Информационно-аналитическое агентство «Телеком-Дэйли». URL: https://telecomdaily.ru/news/2022/06/16/iaa-telecomdaily-v-2023-rynok-va-mozhet-vyrasti-v-dva-raza/ (дата обращения: 09.04.2024)
4. Губеев Э.П. Перспективы развития городской инфраструктуры для улучшения качества жизни // Вестник науки. 2023. №7 (64). С. 245-266.
5. Popular CCTV Camera Brands – JVSG Ratings. URL: https://www.jvsg.com/ipica-ratings/ (дата обращения: 09.04.2024)
6. Kaliuta K. Integration of AI for Routine Tasks Using Salesforce // Asian Journal of Research in Computer Science. 2023. Vol. 16(3). P. 119-127.
7. IP Camera Market by Component (Hardware, Services), Product Type (Fixed, Pan-Tilt-Zoom (PTZ), Infrared), Connection Type (Consolidated, Distributed), Application (Residential, Commercial, Government), and Region 2024-2032. URL: https://www.imarcgroup.com/ip-camera-market#:~:text=The%20global%20IP%20camera%20market,key%20factors%20driving%20the%20market (дата обращения: 08.04.2024)
8. Speed camera statistics. URL: https://www.scdb.info/en/stats/ (дата обращения: 08.04.2024)
9. Фролова Е. Ю., Кошлыкова Ю.А. Идентификация человека по биометрическим данным: обзор современных технологий // Северо-Кавказский юридический вестник. 2022. №3. С. 167-174.
10. Космачева И.М., Кучин И.Ю., Давидюк Н.В., Руденко М.Ф., Лобейко В.И., Сибикина И.В. Система событийного мониторинга для автоматизированного обнаружения инцидентов // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2023. №. 3. С. 76-86.
11. Накиев Р.Р., Ульянов В.В. Анализ уязвимостей Интернета вещей (IoT) и способы их предотвращения // Вестник науки. 2023. Т. 4. №. 7 (64). С. 250-264.

12. RCE Vulnerability in Hikvision Cameras. URL: https://www.cisa.gov/news-events/alerts/2021/09/28/rce-vulnerability-hikvision-cameras-cve-2021-36260 (дата обращения: 11.04.2024)
13. USN-5889-1: ZoneMinder vulnerabilities / Linux. URL: https://www.linuxcompatible.org/story/usn58891-zoneminder-vulnerabilities/ (дата обращения: 11.04.2024)
14. Киберитоги 2022 года по версии «Информзащиты». URL: https://www.infosec.ru/press-center/news/kiberitogi-2022-goda-po-versii-informzashchity/ (дата обращения: 02.04.2024)
15. Исрафилов А. Кибератаки: масштабы и возможные последствия вирусов, созданных хакерами для компьютеров и телефонов // Тенденции развития науки и образования. 2024. №106(11). С. 48-52.
16. Яковишин А.Д. Борьба с перехватом трафика RFID и дистанционного управления: методы защиты и повышение безопасности // Современные научные исследования и инновации. 2024. № 1. https://web.snauka.ru/issues/2024/01/101405
17. Security startup Verkada hack exposes 150,000 security cameras in Tesla factories, jails, and more / Verkada. URL: https://www.theverge.com/2021/3/9/22322122/verkada-hack-150000-security-cameras-tesla-factory-cloudflare-jails-hospitals (дата обращения: 02.04.2024)
18. Number of households with smart security cameras worldwide from 2016 to 2027 // Statista. URL: https://www.statista.com/forecasts/1301193/worldwide-smart-security-camera-homes (дата обращения: 12.04.2024)
19. Amazon Quickly Fixed a Vulnerability in Ring Android App That Could Expose Users' Camera Recordings / Checkmarx. URL: https://www.statista.com/forecasts/1301193/worldwide-smart-security-camera-homes (дата обращения: 12.04.2024)
20. U.S. Department of Justice Disrupts Hive Ransomware Variant. URL: https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant (дата обращения: 05.04.2024)
21. В России научились защищать системы интеллектуального видеонаблюдения от кибератак / Национальный портал в сфере искусственно-

го интеллекта. URL: https://ai.gov.ru/mediacenter/v-rossii-nauchilis-zashchishchat-sistemy-intellektualnogo-videonablyudeniya-ot-kiberatak/ (дата обращения: 05.04.2024)
22. Герасимов А. С. Основные проблемы информационной сетевой безопасности и варианты борьбы с ними // Актуальные исследования. 2022. №40 (119). https://apni.ru/article/5662-osnovnie-problemi-informatsionnoj-setevoj-bez
23. Man Wrongfully Arrested Because Face Recognition Can't Tell People Apart / Aclu Press Releases. URL: https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant (дата обращения: 12.04.2024)
24. Более миллиона камер установлены в России для наблюдения за безопасностью / Национальный портал в сфере искусственного интеллекта. URL: https://ai.gov.ru/mediacenter/glava-mintsifry-maksut-shadaev-zayavil-chto-kazhdaya-tretya-kamera-sledyashchaya-za-bezopasnostyu-v-/ (дата обращения: 08.04.2024)
25. Grepan V. Theoretical and practical foundations of smart contract validation // Innovacionnaya nauka. 2024. №3-2. P. 24-28.
26. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. URL: https://www.iso.org/standard/27001 (дата обращения: 13.04.2024)
27. Котлярова Е. В., Волохова Е. А. Архитектурно-градостроительные особенности редевелопмента бывших промышленных зон на примере Канэри-Уорф в Лондоне // Цифровизация: новые тренды и опыт внедрения: сборник статей. 2023. С. 128.

References

1. Video Surveillance Market Size & Share Analysis - Growth Trends & Forecasts (2024-2029). URL: https://www.mordorintelligence.com/industry-reports/video-surveillance-systems-market (accessed 05.04.2024)
2. Surveillance camera statistics / Surveillance Studies. URL: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ (accessed 02.04.2024).

3. IAA TelecomDaily: IA market can grow twice / Information and Analytical Agency “Telecom-Daily”. URL: https://telecomdaily.ru/news/2022/06/16/iaa-telecomdaily-v-2023-rynok-va-mozhet-vyrasti-v-dva-raza/ (accessed 09.04.2024)
4. Gubeev E.P. Prospects for the development of urban infrastructure to improve the quality of life. *Vestnik nauki*, 2023, no. 7 (64), pp. 245-266.
5. Popular CCTV Camera Brands - JVSG Ratings. URL: https://www.jvsg.com/ipica-ratings/ (accessed 09.04.2024)
6. Kaliuta K. Integration of AI for Routine Tasks Using Salesforce. *Asian Journal of Research in Computer Science,* 2023, vol. 16(3), pp. 119-127.
7. IP Camera Market by Component (Hardware, Services), Product Type (Fixed, Pan-Tilt-Zoom (PTZ), Infrared), Connection Type (Consolidated, Distributed), Application (Residential, Commercial, Government), and Region 2024-2032. URL: https://www.imarcgroup.com/ip-camera-market#:~:text=The%20global%20IP%20camera%20market,key%20factors%20driving%20the%20market (accessed 08.04.2024)
8. Speed camera statistics. URL: https://www.scdb.info/en/stats/ (accessed 08.04.2024)
9. Frolova E. Y., Koshlykova Y.A. Human identification by biometric data: a review of modern technologies. *North Caucasian Legal Bulletin,* 2022, no. 3, pp. 167-174.
10. Kosmacheva, I.M.; Kuchin, I.Yu.; Davidyuk, N.V.; Rudenko, M.F.; Lobeiko, V.I.; Sibikina, I.V. Event monitoring system for automated incident detection. *Bulletin of Astrakhan State Technical University. Series: Management, Computer Science and Informatics,* 2023, no. 3, pp. 76-86.
11. Nakiev R.R., Ulyanov V.V. Analysis of the Internet of Things (IoT) vulnerabilities and ways to prevent them. *Vestnik nauki,* 2023, vol. 4, no. 7 (64), pp. 250-264.
12. RCE Vulnerability in Hikvision Cameras. URL: https://www.cisa.gov/news-events/alerts/2021/09/28/rce-vulnerability-hikvision-cameras-cve-2021-36260 (accessed 11.04.2024)

13. USN-5889-1: ZoneMinder vulnerabilities / Linux. URL: https://www.linuxcompatible.org/story/usn58891-zoneminder-vulnerabilities/ (accessed 11.04.2024)
14. CyberTogs of 2022 according to Informzaschita. URL: https://www.infosec.ru/press-center/news/kiberitogi-2022-goda-po-versii-informzashchity/ (accessed 02.04.2024)
15. Israfilov A. Cyberattacks: the scale and possible consequences of viruses created by hackers for computers and phones. *Trends in the development of science and education,* 2024, no. 106(11), pp. 48-52.
16. Yakovishin A.D. Combating the interception of RFID and remote control traffic: methods of protection and security enhancement. *Modern Scientific Research and Innovations,* 2024, no. 1. https://web.snauka.ru/issues/2024/01/101405
17. Security startup Verkada hack exposes 150,000 security cameras in Tesla factories, jails, and more / Verkada. URL: https://www.theverge.com/2021/3/9/22322122/verkada-hack-150000-security-cameras-tesla-factory-cloudflare-jails-hospitals (accessed 02.04.2024)
18. Number of households with smart security cameras worldwide from 2016 to 2027 / Statista. URL: https://www.statista.com/forecasts/1301193/worldwide-smart-security-camera-homes (accessed 12.04.2024)
19. Amazon Quickly Fixed a Vulnerability in Ring Android App That Could Expose Users' Camera Recordings / Checkmarx. URL: https://www.statista.com/forecasts/1301193/worldwide-smart-security-camera-homes (accessed on 12.04.2024)
20. U.S. Department of Justice Disrupts Hive Ransomware Variant. URL: https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant (accessed 05.04.2024)
21. Russia has learned to protect intelligent video surveillance systems from cyberattacks / National portal in the field of artificial intelligence. URL: https://ai.gov.ru/mediacenter/v-rossii-nauchilis-zashchishchat-sistemy-intellektualnogo-videonablyudeniya-ot-kiberatak/ (accessed 05.04.2024)
22. Gerasimov A. S. Main problems of information network security and options to combat them. *Actual researches,* 2022, no. 40 (119). https://apni.ru/article/5662-osnovnie-problemi-informatsionnoj-setevoj-bez

23. Man Wrongfully Arrested Because Face Recognition Can't Tell People Apart / Aclu Press Releases. URL: https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant (accessed 12.04.2024)
24. More than one million cameras installed in Russia for security surveillance / National portal in the field of artificial intelligence. URL: https://ai.gov.ru/mediacenter/glava-mintsifry-maksut-shadaev-zayavil-chto-kazhdaya-tretya-kamera-sledyashchaya-za-bezopasnostyu-v-/ (accessed 08.04.2024)
25. Grepan V. Theoretical and practical foundations of smart contract validation. *Innovacionnaya nauka,* 2024, no. 3-2, pp. 24-28.
26. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. URL: https://www.iso.org/standard/27001 (accessed 13.04.2024)
27. Kotlyarova E. V., Volokhova E. A. Architectural and urban planning features of redevelopment of former industrial zones on the example of Canary Wharf in London. *Digitalization: new trends and experience of implementation: a collection of articles,* 2023, p. 128.

ДАННЫЕ ОБ АВТОРАХ

Анар Исрафилов, индивидуальный исследователь
israfilov_anar@ro.ru

Ситников Павел Романович, бакалавр
Московский государственный технический университет им. Н. Э. Баумана
ул. 2-я Бауманская, 5, Москва,105005, Российская Федерация
sitnikov_p@mail.ru

Соколов Александр Денисович, бакалавр
Московский государственный технический университет им. Н. Э. Баумана
ул. 2-я Бауманская, 5, Москва,105005, Российская Федерация
sokolov_alex@mail.ru

Ишанхонов Азизхон Юнусхон угли, магистр
Университет науки и технологий МИСИС
Ленинский пр-кт, 4, стр. 1., Москва, 119049, Российская Федерация
ishanaziz@ya.ru

Благова Ирина Юрьевна, к.э.н., доцент
Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого»
ул. Политехническая, 29, Санкт-Петербург, 195251, Российская Федерация
blagovairina@ya.ru

DATA ABOUT THE AUTHORS

Anar Israfilov, individual researcher
israfilov_anar@ro.ru
ORCID: https://orcid.org/0009-0004-5760-9631

Pavel R. Sitnikov, bachelor's degree
Bauman Moscow State Technical University
5, 2nd Baumanskaya Str., Moscow, 105005, Russian Federation
sitnikov_p@mail.ru
ORCID: https://orcid.org/0009-0000-0960-4108

Aleksandr D. Sokolov, bachelor's degree
Bauman Moscow State Technical University
5, 2nd Baumanskaya Str., Moscow, 105005, Russian Federation
sokolov_alex@mail.ru
ORCID: https://orcid.org/0009-0002-7336-9573

Azizkhon Yu. Ishankhonov, master's degree
The National University of Science and Technology MISIS
4, Leninskiy Prospekt, Moscow, 119049, Russian Federation

ishanaziz@ya.ru
ORCID: https://orcid.org/0009-0009-8934-6289

Irina Yu. Blagova, PhD, Associate Professor
Peter the Great St.Petersburg Polytechnic University
29, Politekhnicheskaya Str., St. Petersburg, 195251, Russian Federation
blagovairina@ya.ru
ORCID: https://orcid.org/0000-0002-2418-1702

Поступила 14.05.2024
После рецензирования 01.06.2024
Принята 05.06.2024

Received 14.05.2024
Revised 01.06.2024
Accepted 05.06.2024