ТЕХНИЧЕСКИЕ НАУКИ | TECHNICAL SCIENCES

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
INFORMATICS, COMPUTER ENGINEERING AND MANAGEMENT

Современная наука и инновации. 2025. № 3. С. 10-19.
ТЕХНИЧЕСКИЕ НАУКИ
ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Modern Science and Innovations. 2025;(3):10-19.
TECHNICAL SCIENCE
INFORMATICS, COMPUTER ENGINEERING AND MANAGEMENT

Научная статья
УДК 004.418
https://doi.org/10.37493/2307-910X.2025.3.1

Кибербезопасность биометрических хранилищ на спортивных объектах и необратимость утечек

Саяпов Альберт Альбертович[1*]

[1] FIFA, Майами, США
[1] scholar@sayapov.net, ORCID: 0009-0008-8260-0531

*** Автор, ответственный за переписку**

Аннотация. Введение. *В статье рассматривается кибербезопасность биометрических хранилищ на спортивных объектах с целью оценить природу и последствия утечек, установить степень необратимости компрометации биометрических шаблонов и предложить практические меры уменьшения рисков.* ***Материалы и методы****. Исследование опирается на сравнительный анализ архитектур хранения, разбор документированных инцидентов (включая массовые утечки верификационных платформ), обзор регуляторных требований и данные о векторах атак в многоузловых инфраструктурах. Актуальность работы продиктована массовым внедрением «лицо-как-пропуск» и интеграцией биометрии в платежи и программы лояльности, что трансформирует турникет в центральный узел коммерческого и идентификационного риска; показано, что современные методы реконструкции из хешированных векторов и широкие возможности перекрёстного сопоставления делают компрометацию долгосрочной и системной.* ***Результаты и обсуждение****. Новизна состоит в синтезе эмпирики утечек и технологического анализа с предложением прикладной архитектуры защиты — сочетания отзывной токенизации, аппаратного хранения ключей и сверки в защищённых вычислительных зонах — и в продуктовой формулировке комплекса организационных мер (микросегментация, red-team, контрактная дисциплина, минимизация данных).* ***Заключение****. Биометрические шаблоны образуют критическую «точку отказа», ущерб от которой носит кумулятивный и практически необратимый характер; технические контрмеры без устойчивых организационных практик и постоянного управления риском недостаточны. Статья будет полезна операторам арен, поставщикам биометрических решений, командам кибербезопасности, регуляторам и исследователям в области приватности.*

Ключевые слова: биометрические хранилища, стадионы, утечка данных, необратимость, токенизация, микросегментация, аппаратные криптомодули

Для цитирования: *Саяпов А. А. Кибербезопасность биометрических хранилищ на спортивных объектах и необратимость утечек // Современная наука и инновации. 2025. №3. С. 10-19. https://doi.org/10.37493/2307-910X.2025.3.1*

Research article

Cybersecurity of biometric data storage at sports facilities and the irreversibility of leaks

Albert A. Sayapov[1*]

[1] FIFA, Miami, USA

[1] scholar@sayapov.net, ORCID: 0009-0008-8260-0531

*** Corresponding author**

Abstract. Introduction. *This article examines the cybersecurity of biometric storage systems at sports venues with the aim of assessing the nature and consequences of leaks, establishing the degree of irreversibility of biometric template compromise, and proposing practical risk mitigation measures.* ***Materials and methods.*** *The study is based on a comparative analysis of storage architectures, a review of documented incidents (including massive leaks of verification platforms), a review of regulatory requirements, and data on attack vectors in multi-node infrastructures. The relevance of this work is dictated by the widespread adoption of "face-as-pass" systems and the integration of biometrics into payments and loyalty programs, which transforms the turnstile into a central hub for commercial and identification risk. It is shown that modern methods of reconstruction from hashed vectors and extensive cross-matching capabilities make compromises long-term and systemic.* ***Results and discussion.*** *The novelty lies in the synthesis of leak empirical data and technological analysis, with a proposal for an applied security architecture—a combination of revocable tokenization, hardware-based key storage, and verification in secure computing areas—and a product-based formulation of a set of organizational measures (microsegmentation, red-teaming, contractual discipline, and data minimization).* ***Conclusion.*** *The key conclusion is that biometric templates form a critical "point of failure," the damage from which is cumulative and virtually irreversible; technical countermeasures without robust organizational practices and ongoing risk management are insufficient. This article will be useful for arena operators, biometric solution providers, cybersecurity teams, regulators, and privacy researchers.*

Keywords: biometric storage, stadiums, data leakage, irreversibility, tokenization, microsegmentation, hardware crypto modules

For citation: *Sayapov AA. Cybersecurity of biometric data storage at sports facilities and the irreversibility of leaks. Modern science and innovation. 2025;(3):10-19. (In Russ.). https://doi.org/10.37493/2307-910X.2025.3.1*

Введение. В дни проведения матчей физический проход болельщика через турникет всё чаще реализуется с помощью биометрической идентификации: алгоритм извлекает двумерный вектор признаков лицевого изображения, сопоставляет его с персональным онлайн-профилем, после чего доступ предоставляется без предъявления телефона или бумажного билета. Парадигма «лицо-как-пропуск» трансформирует операционную экономику стадиона: входной трафик переводится в управляемый цифровой поток, измеряемый в миллисекундах, а каждое сканирование одновременно обогащает данные маркетинговой базы данных. Соответственно, к началу сезона 2025 года по меньшей мере шесть клубов MLB интегрировали в приложение Ballpark опцию Go-Ahead Entry, позволяющую зрителям проходить через выделенную линию без дополнительного досмотра; этой функцией уже пользуются тысячи посетителей на каждой домашней серии игр [1].

Скорость, бесконтактность и борьба с мошенничеством — основные драйверы развития биометрии. Системы Wicket, используемые командой Cleveland Browns и несколькими другими командами, обеспечивают среднее время прохода примерно 2 секунды на человека; по оценке клуба, это позволило в среднем освобождать входные зоны примерно на 10 минут быстрее по сравнению с традиционными методами сканирования, что важно для телевизионного хронометража и операций в антракте [2]. По

сути, турникет становится всего лишь ещё одним узлом в системе «умного» отслеживания контактов: тот же самый шаблон лица можно использовать для покупки хот-дога или подтверждения возраста при покупке пива, превращая распознавание в ещё одну транзакцию.

Скорость едва ли убедила бы регуляторов, если бы не вопрос безопасности. После серии инцидентов с пиротехникой и массовыми драками силовые ведомства требуют точной идентификации нарушителей. Для дирекции арен это дополнительный аргумент: один аппаратный канал решает две задачи—ускоряет потоки и снижает правовые риски.

Такие системы в основном состоят из трех компонентов. Мобильное приложение или веб-портал отвечает за «посадку» — процесс первичной регистрации, в ходе которого биометрические данные пользователя привязываются к его учётной записи: изображение лица пользователя конвертируется в черновой шаблон и передаётся на облачный сервер, где происходит обработка и сопоставление биометрических данных с помощью специализированных алгоритмов. На стадионе расположена группа edge-камер либо embedded-планшетов у турникетов; они выполняют предварительный анализ данных на самом устройстве, включающий проверку на “живость” для противодействия имитационным атакам и оценку качества лицевого изображения в режиме реального времени, шифруют уникальный математический отпечаток (вектор) и отправляют его на верификацию. Хранение цифровых ID в одной платформе для VIP-лож, POS-расчётов и программ лояльности уменьшает число аппаратных точек отказа и поддерживает модель «один профиль — много сервисов», применяемую в NEC I: Delight и аналогичных решениях [3].

Таким образом, технология уже переросла экспериментальную стадию: она интегрирована в физическую структуру современных арен. Дальнейшее обсуждение о рисках и обратимости утечек не может быть отделено от того, что биометрические данные стали неотделимой частью доступа, монетизации и правоприменения в спорте—и любая компрометация этого цикла равна компрометации самой модели выручки стадиона.

Материалы и методология. Материалы и методология исследования опираются на сочетание академических источников, отраслевых отчётов, регуляторных документов и эмпирических кейсов утечек, что позволяет рассматривать проблему биометрической безопасности спортивных объектов в комплексной перспективе. Теоретическая база формируется работами, фиксирующими внедрение биометрии в инфраструктуру стадионов и её экономический эффект: исследование Haskins [1] раскрывает трансформацию турникета в узел сбора данных и маркетинговую CRM, а Kapustka [2] демонстрирует рост скорости идентификации и влияние на коммерческую логику матч-дня. Отдельный пласт составляют технологические обзоры поставщиков решений, включая NEC [3], что позволяет реконструировать типовую архитектуру хранилища и потоков данных.

Ключевой эмпирический материал основан на задокументированных инцидентах, связанных со взломом: крупномасштабная утечка BioStar 2, о которой сообщила газета Guardian [4], а затем последовавшая за ней утечка из платформы Outabox [5] доказывают, что при уязвимости унифицированных баз данных биометрические шаблоны становятся универсальным идентификатором для злоумышленников. В данной статье эти случаи используются в качестве контрольных точек, доказывающих необратимость утечек на практике. Системное понимание угроз дополняется отчётом ENISA 2023 [6], в котором зафиксирован рост числа атак на многоузловые сценарии, включающих как социальную инженерию, так и уязвимости в облаке, а также подмену данных на периферийных устройствах.

Методологически исследование объединяет три аналитических траектории. Первая — сравнительный анализ архитектурных решений: от классической централизованной базы до гибридных схем с отзывными токенами и аппаратными криптомодулями, что позволяет оценить эффективность «двойной капсулы» защиты. Вторая —

систематический обзор регуляторных норм: положения GDPR [18], проект AI Act [19] и международный стандарт ISO/IEC 30107-3 [20] дают рамку для понимания правовой природы риска и закрепляют обязательность мер против имитационных атак. Третья — контент-анализ социологических и рыночных опросов: данные Европейского центрального банка [16] о предпочтениях в аутентификации и опрос Stadium Tech Report [17] о реальном внедрении биометрии на аренах демонстрируют амбивалентность между удобством и недоверием.

Результаты и обсуждение. К удобству, описанному в предыдущем разделе, спортивные объекты подошли через призму доверия к уникальным телесным признакам зрителя, однако та же концентрация данных, что ускоряет проход, превращает биометрическое хранилище в критически уязвимый слой инфраструктуры. Когда шаблоны лица и отпечатков собираются в одной базе, сама идея «единственной уязвимой точки» перестаёт быть метафорой: в случае утечки оператор фактически передаёт злоумышленнику «ключ» от любого турникета, кассы самообслуживания и VIP-зоны. Так было с системой BioStar 2, где исследователи нашли 27,8 млн записей, включая отпечатки и пароли администраторов в открытом виде; данные касались более миллиона персон, а изменить их можно было удалённо, что позволяло злоумышленнику привязать свой отпечаток к чужой учётной записи и беспрепятственно проходить на объект [4]. Пятилетие спустя история повторилась: взлом платформы Outabox раскрыл свыше миллиона лицевых векторов и даже сканы водительских удостоверений посетителей арен Австралии, США и Филиппин, продемонстрировав, что шаг от клубов к стадионам минимален и администрируется теми же разработчиками с теми же практиками доступа «все в одном Excel» [5].

Даже когда центральная база защищена, сквозная цепочка сбора и проверки работает раздельно: мобильное приложение интегрируется с облаком, камеры на входе — с локальной сетью, а подрядчик по общественному питанию подключается через API с отдельным набором ключей. Анализ ENISA за 2023 год показал, что именно в таких многоузловых сценариях растёт доля атак, комбинирующих социальную инженерию, уязвимости в облачных сервисах и подмену данных на периферийных устройствах, причём социальная инженерия вышла в пятерку наиболее динамично растущих угроз за отчётный период, что показано на рисунке 1 [6]. Практика показывает: хакеру порой достаточно перехватить слабозащищённый поток RTSP-камеры у точки общественного питания, чтобы извлечь хеш вектора и по цепочке добраться до защищённого ядра, где этот же вектор хранится в более строгом виде.

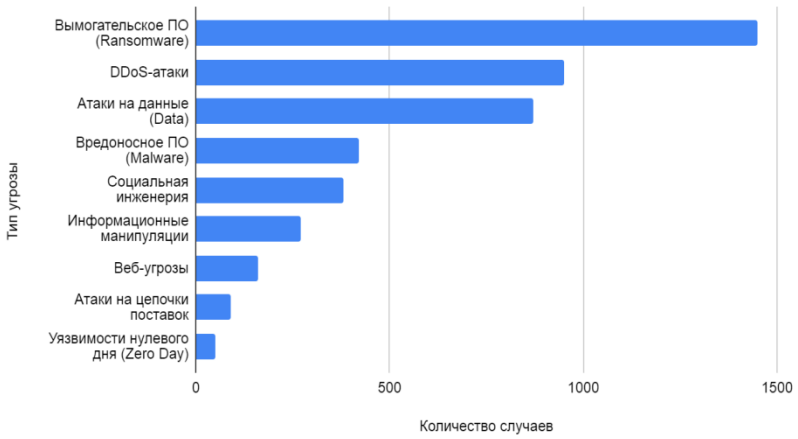

Рисунок 1. Наблюдаемые события, связанные с основными угрозами ETL в разрезе затронутого сектора [6]

Figure 1. Observed events related to the main ETL threats by affected sector [6]

Дополнительный слой риска создаёт перекрёстное использование шаблонов. На современных аренах один и тот же биометрический вектор открывает турникет, оплачивает напиток и подтверждает возраст. Таким образом, компрометация доступа автоматически означает компрометацию финансовой транзакции. Как показано на рисунке 2, большинство респондентов в еврозоне (≈50%) предпочитает многофакторную аутентификацию при онлайн-платежах, тогда как однофакторные решения и биометрия выбираются примерно четвертью населения каждая, что указывает на склонность к безопасности при сохранении относительной популярности удобных схем [16].

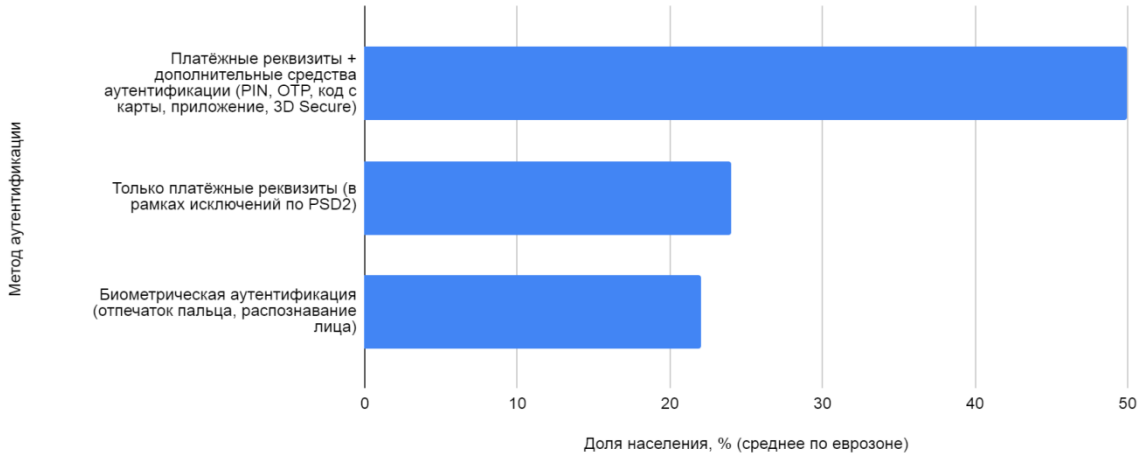

Рисунок 2. Предпочтения методов аутентификации при онлайн-платежах в еврозоне [16]
Fig. 2. Preferences for authentication methods in online payments in the eurozone [16]

Американские сенаторы в 2021 году выражали опасения по поводу Amazon One, указывая, что изображения шифруются, но всё равно уходят в облако Amazon, а значит становятся доступными для анализа в рекламных целях и в случае будущей утечки могут быть увязаны с покупательскими привычками клиента [7]. В спортивной индустрии, где программы лояльности уже объединяют билет, мерч и питание, подобный «сквозной слепок» личности оказывается ещё более ценным — и для маркетолога, и для мошенника. Как показано на рисунке 3, 58% опрошенных стадионов не используют биометрию; среди тех, кто внедряет технологию, основной кейс — внутренний доступ для персонала и медиа (37%), тогда как массовое клиентское применение для прохода, премиум-зон и точек питания остаётся редким (14%, 8% и 7% соответственно), что указывает на консервативный и селективный характер внедрения [17].

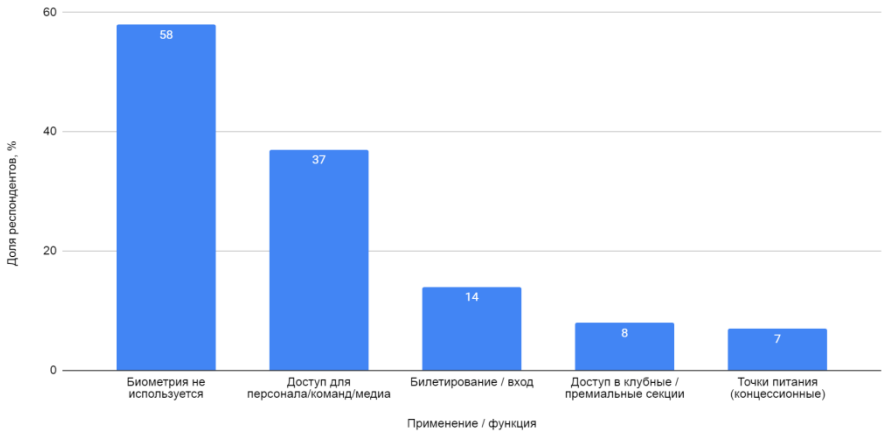

Рисунок 3. Распределение функциональных применений биометрической аутентификации в стадионной инфраструктуре [17]
Fig. 3. Distribution of functional applications of biometric authentication in stadium infrastructure [17]

Однако это приобретает новые формы имитации. «Презентационные атаки» — поддельные маски из силикона, высокоточные распечатки лица, синтетическое видео — всё чаще выходят за пределы лабораторий. Отчёт Европола 2025 года фиксирует, что идентификацию можно обмануть не только глянцевой фотографией, но и динамической «глубокой подделкой», которая на уровне пикселей повторяет микродвижения живого лица [8]. Отсюда возникает ситуация, когда разработчики включают детекторы «живости» и анализ мерцания кожи, но злоумышленники отвечают улучшенными латексными матрицами и генерацией фазовых шумов, которые имитируют кровоток под инфракрасными датчиками [9]. Академические работы по периокулярной аутентификации подтверждают, что при ограничении качества видеопотока до уровня обычной стадионной камеры глубокая подделка сохраняет 30-процентный шанс пройти без срабатывания защиты, особенно если прежний шаблон добыт из того же хранилища и учтены индивидуальные особенности моргания [10].

Таким образом, то, что начиналось как ускоритель болельщицкого опыта, превращается в конденсатор уязвимостей: единая база, разноуровневая защита узлов, совмещение физического доступа и платежей и, наконец, нарастающая волна имитационных атак образуют четыре грани одной пирамиды рисков. Пока лига экономит секунды на турникетах, злоумышленник экономит месяцы на подготовку — ведь, заполучив необратимый биометрический ключ, он получает входной билет не только на конкретный стадион, но и в цифровую жизнь человека.

Биометрические утечки опасны, прежде всего, тем, что если пароль или пластиковую карту можно сменить, то к биометрии это неприменимо. Юридические исследования подчёркивают: в отличие от имени или номера социального страхования, биометрические признаки физически закреплены за человеком и, оказавшись в сети, остаются там навсегда; потеряв контроль над ними, человек не имеет реальной возможности «сменить лицо» или отпечаток и тем самым обнулить риск [11].

Необратимость усиливается техническим прогрессом. В мае 2025-го группа исследователей из Сингапура и Республики Корея показала, что из 512-значного вектора — того самого «захешированного» шаблона, который операторы стадионов считают безопасным — можно за сотню запросов восстановить визуально узнаваемый портрет болельщика. Скорость атаки выросла в тысячи раз против прежних оценок, что превращает любые скомпрометированные шаблоны в сырой материал для подделок, способных пройти сквозь камеры турникетов и системы бесконтактной оплаты [12].

После утечки биометрия мгновенно соединяется с открытыми источниками. Ещё в эксперименте Карнеги-Меллон незнакомцев, идущих по кампусу, распознавали «по-фейсбуку» и дополняли досье скрытой персональной информацией, включая элементы социального номера [13]. С тех пор точность только растёт: современные алгоритмы связывают разрозненные аккаунты по траекториям перемещений и сетевому трафику с вероятностью свыше 85% — достаточно, чтобы фотография с камеры стадиона автоматически подтянула к болельщику историю покупок и политических лайков [14]. Таким образом, единичная утечка стремительно расширяется до «композитного» профиля, объединяющего офлайн- и онлайн-компоненты.

Усугубляет ситуацию латентность злоупотреблений: компании в среднем обнаруживают и локализуют взлом лишь через 241 день после его начала, и это лучший показатель за последние девять лет по данным глобального отчёта IBM 2025 года [15]. Для спортивной арены это означает почти целый сезон матчей, в течение которого злоумышленник может ходить на игры, совершать покупки и копить «белую» историю лояльного фаната, пока владельцы системы уверены, что всё под контролем.

Совокупность новизны самого биометрического признака, возможности восстановления облика по его числовому «отпечатку», высокой степени совпадения с открытыми массивами данных и длительных периодов незаметной циркуляции образуют

замкнутую петлю риска. Стоит такому вектору выйти за пределы контролируемого периметра, как он мгновенно утрачивает временный статус и превращается в устойчивый маркер личности, к которому будут присоединяться новые компрометации, фрагменты социальных сетей и следы финансовых операций. Для администраторов стадионов это означает необходимость непрерывной и превентивной защиты: в противном случае цифровая тень болельщика будет преследовать его куда дольше, чем действуют билеты или сезонные пропуска.

Европейское право трактует биометрию как особо чувствительную категорию: статья 9 Общего регламента о защите данных запрещает её обработку без явного согласия либо весомого общественного основания и требует предварительной оценки воздействия на приватность [18]. Акт ЕС об искусственном интеллекте относит системы доступа на стадионы к «высокорисковым» и обязывает операторов вести постоянное управление риском, фиксировать точность алгоритма и сообщать о происшествиях в надзорный орган [19].

Международный стандарт ISO/IEC 30107-3 закрепляет методику оценки устойчивости к «презентационным атакам»; его прохождение становится де-факто лицензией для вендора, поскольку регуляторы и страховые компании принимают только решения с документированным уровнем сопротивления подделкам [20]. Таким образом, регуляторное поле быстро сходится к общему знаменателю: строгая правовая защита, обязательная проверка живости и материальные санкции за любую утечку, что делает кибербезопасность биометрического хранилища не столько технической, сколько правовой необходимостью.

Чтобы прервать цепочку уязвимостей инфраструктура стадиона должна быть разделена на маленькие изолированные фрагменты. Недоверительная модель требует рассматривать каждый узел — турникет, камеру, кассу, облачный контейнер — как потенциально враждебный; потому между ними поднимаются микросегменты, сквозь которые трафик проходит лишь при строгой проверке подлинности и минимальных привилегиях. Такой подход ломает традиционную логику периметра: даже если злоумышленник получит доступ к одному фрагменту сети, он упрётся в стену, когда попытается перескочить в соседний.

Физическую нерушимость шаблонов обеспечивает переход от единого «главного сейфа» к гибридной схеме: сами шаблоны хранятся в форме отзывных токенов, которые можно заново сгенерировать при подозрении на компрометацию, а ключи шифрования запираются в аппаратных криптомодулях. В точке сверки следует применять либо полностью гомоморфное шифрование, позволяющее сопоставлять векторы, не раскрывая их содержимого, либо перенос вычислений в доверенную область самого процессора, где постороннее программное обеспечение ничего не увидит. Получается двойная капсула: одни данные взаимозаменяемы, другие аппаратно недоступны.

Однако это остается теорией без постоянного давления извне. Поэтому раз в квартал на арену приглашаются команды имитационных атак, которые ищут лазейки так же, как это сделал бы реальный похититель биометрии, а найденные изъяны оплачиваются через программу стимулирования исследователей. Так обнаруживаются неочевидные дыры: например, устаревшая прошивка инфракрасного датчика или неправильно настроенный список разрешений в контейнере с журналами. Параллельно действует автоматическое правило минимизации: всё, что не нужно именно сейчас, удаляется или псевдонимизируется, а каждый временной штамп запускает таймер, по истечении которого данные исчезают без ручного участия.

С точки зрения управленца клубом этой технике отвечает организационный маршрут. Сначала составляется карта, где стрелками указано, откуда и куда движется каждый фрагмент информации болельщика. Такое упражнение сразу выявляет лишние копии и неожиданные точки слияния потоков. Затем контракты с поставщиками наполняются строгими требованиями по доступности, шифрованию и времени реакции на

инцидент, иначе сотрудничество будет считаться несостоявшимся. На практическом уровне зрителю дают возможность выбрать запасной способ входа — пусть это одноразовый двумерный код или бесконтактный токен; отказ от биометрии не должен превращать поход на матч в квест. И наконец, люди. Операторы турникетов, продавцы в киосках, администраторы сети проходят регулярные тренировки и учатся видеть не только лицо клиента, но и сценарий атаки, прячущийся за приветливой улыбкой. Тактика и технологии сходятся в одной точке, то есть цифровая стена обретает пульсирующее саморегулирующееся сердце. По сути, синтез достигается за счёт объединения технологий. Использование логических барьеров в сочетании с правилами управления порождает разветвлённую многоуровневую конфигурацию безопасности, в которой отказ или уязвимость одного узла больше не приводит к краху всей цепи. Хранилище уже перестало быть «местом окончательного доверия», превратившись в определённую экосистему, динамично реагирующую на новые атаки и локализующую ущерб даже при частичной компрометации. Поэтому статическая модель должна трансформироваться в самообучающуюся архитектуру, что является ещё одним условием решения главной проблемы — необратимости утечек, поскольку только в этом случае данные болельщиков не становятся заложниками инфраструктурных ошибок, сохраняя при этом возможность контролируемого использования в будущем.

Заключение. Анализ продемонстрированных инцидентов и динамики угроз приводит к однозначному выводу: внедрение биометрии в стадионную инфраструктуру трансформировало турникет и сопутствующие сервисы из вспомогательных узлов в критически важные центры сбора и сшивки персональных данных, где концентрация шаблонов лица и отпечатков создаёт «единичную уязвимую точку» с исключительно высокой ценностью для злоумышленника. Примеры массовых утечек и эксплойтов, способность реконструировать визуально узнаваемые портреты из хешированных векторов, а также высокий уровень перекрёстного сопоставления с открытыми источниками превращают любую компрометацию не просто в локальный инцидент, а в начало непрерывного процесса наростающих связей между офлайн- и онлайн-профилями человека. Биометрические характеристики не могут быть обращены вспять, и поскольку могут пройти месяцы, прежде чем атака будет обнаружена, ущерб конфиденциальности и коммерческим моделям оператора может сохраняться гораздо дольше, чем один спортивный сезон.

Технические меры без организационных регламентов остаются недостаточными, как и формальные требования к шифрованию без проверки всего пути передачи данных. Архитектурные принципы недоверия и микросегментации, отказ от единого «главного сейфа» в пользу схем с передаваемыми и отзывными маркерами, хранение ключей в аппаратных криптомодулях, использование методов, позволяющих верифицировать векторы без раскрытия их содержимого – как гомоморфным шифрованием, так и переносом вычислений в доверенные области процессора – становятся практически оправданными. Эта техническая «двойная капсула» должна дополняться регулярными имитационными атаками и программами вознаграждений для исследователей, строгой политикой минимизации и псевдонимизации, а также контрактной дисциплиной в отношении поставщиков и резервными способами доступа для болельщика, чтобы отказ от биометрии не превращал посещение матча в препятствие.

Именно сочетание перечисленных технических мер и устойчивых организационных практик делает возможным переход от статической модели защиты к непрерывно обучающейся архитектуре, способной сокращать последствия компрометаций и частично нивелировать эффект необратимости утечек. Для владельцев арен это означает необходимость системного, проактивного подхода: защита биометрических хранилищ должна рассматриваться не как разовая задача по соответствию требованиям, а как непрерывный процесс управления риском, без которого каждая новая секунда ускорения

прохода будет стоить уязвимости, преследующей болельщика гораздо дольше, чем действует его абонемент.

ЛИТЕРАТУРА / REFERENCES

1. Haskins C. Stadiums Are Embracing Face Recognition. Privacy Advocates Say They Should Stick to Sports [Электронный ресурс]. WIRED. 21.08.2024. URL: https://www.wired.com/story/face-recognition-stadiums-protest/ (дата обращения: 23.07.2025).
2. Kapustka P. Wicket's facial authentication technology a ticket to success for Cleveland Browns [Электронный ресурс]. Stadium Tech Report. 28.02.2024. URL: https://stadiumtechreport.com/feature/wickets-facial-authentication-technology-a-ticket-to-success-for-cleveland-browns/ (дата обращения: 24.07.2025).
3. Introducing NEC's Digital ID For Stadiums And Sporting Arenas [Электронный ресурс]. NECAM. URL: https://www.necam.com/digitalid/stadium/ (дата обращения: 25.07.2025).
4. Taylor J. Major breach found in biometrics system used by banks, UK police and defence firms [Электронный ресурс]. The Guardian. 14.08.2019. URL: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms (дата обращения: 26.07.2025).
5. Pearson J. A Face Recognition Firm That Scans Faces for Bars Got Hacked—and That's Just the Start [Электронный ресурс]. WIRED. 02.05.2024. URL: https://www.wired.com/story/outabox-facial-recognition-breach/ (дата обращения: 27.07.2025).
6. ENISA. ENISA Threat Landscape 2023 [Электронный ресурс]. 2023. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf (дата обращения: 28.07.2025).
7. Reuters. Amazon's palm print recognition raises concern among U.S. senators [Электронный ресурс]. Reuters. 13.08.2021. URL: https://www.reuters.com/technology/amazons-palm-print-recognition-raises-concern-among-by-us-senators-2021-08-13/ (дата обращения: 29.07.2025).
8. Europol. Biometric vulnerabilities: Ensuring future law enforcement preparedness [Электронный ресурс]. 2025. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Biometric-vulnerabilities.pdf (дата обращения: 30.07.2025).
9. Meyer C. No Spoofing: An Introduction to Presentation Attack Detection [Электронный ресурс]. Security Management (ASIS Online). 2024. URL: https://www.asisonline.org/security-management-magazine/articles/2024/08/biometrics/presentation-attack-detection/ (дата обращения: 31.07.2025).
10. Valenzuela A., Tapia J. E., Chang V., Busch C. Presentation Attack Detection using iris periocular visual spectrum images. Frontiers in Imaging. 2024. Т. 3. DOI: 10.3389/fimag.2024.1478783
11. Qandeel M. Facial recognition technology: regulations, rights and the rule of law // Frontiers in Big Data. 2024. Т. 7. DOI: 10.3389/fdata.2024.1354659
12. Burt C. Alarming gains in face reconstruction from biometric templates made by researchers [Электронный ресурс]. Biometric Update. 16.05.2025. URL: https://www.biometricupdate.com/202505/alarming-gains-in-face-reconstruction-from-biometric-templates-made-by-researchers (дата обращения: 01.08.2025).
13. More Than Facial Recognition [Электронный ресурс]. Carnegie Mellon University (CMU). 2011. URL: https://www.cmu.edu/homepage/society/2011/summer/facial-recognition.shtml (дата обращения: 02.08.2025).
14. Senette C., Siino M., Tesconi M. User Identity Linkage on Social Networks: A Review of Modern Techniques and Applications. IEEE Access. 2024. Т. 12. С. 171241–171268. DOI: 10.1109/access.2024.3500374
15. Kessem L. 2025 Cost of a Data Breach Report: Navigating the AI rush without sidelining security [Электронный ресурс]. IBM. 30.07.2025. URL: https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai (дата обращения: 04.08.2025).
16. European Central Bank. Study on the payment attitudes of consumers in the euro area 2024 [Электронный ресурс]. 19.12.2024. URL: https://www.ecb.europa.eu/stats/ecb_surveys/space/html/ecb.space2024~19d46f0f17.en.html?utm_source=chatgpt.com (дата обращения: 05.08.2025).
17. Kapustka P. Survey says: Almost half of venues see biometric technology as a top initiative for 2025 [Электронный ресурс]. Stadium Tech Report. 20.11.2024. URL:

https://stadiumtechreport.com/feature/survey-says-almost-half-of-venues-see-biometric-technology-as-a-top-initiative-for-2025/ (дата обращения: 07.08.2025).

18. Regulation (EU) 2016/679 of the European Parliament and of the Council [Электронный ресурс]. Official Journal of the European Union. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016R0679 (дата обращения: 08.08.2025).

19. European Commission. AI Act [Электронный ресурс]. 2025. URL: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (дата обращения: 09.08.2025).

20. ISO. ISO/IEC 30107-3:2023 [Электронный ресурс]. 2023. URL: https://www.iso.org/standard/79520.html (дата обращения: 09.08.2025.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Саяпов Альберт Альбертович, Менеджер по решениям контроля доступа, FIFA, Майами, США, scholar@sayapov.net, ORCID: 0009-0008-8260-0531

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.
Статья поступила в редакцию 01.08.2025;
одобрена после рецензирования 12.09.2025;
принята к публикации 01.10.2025

INFORMATION ABOUT THE AUTHORS

Albert Sayapov, Access Control Solutions Manager, FIFA, Miami, USA, scholar@sayapov.net, ORCID: 0009-0008-8260-0531

Conflict of interest: the author declare no conflicts of interests.

The article was submitted: 01.08.2025;
approved after reviewing: 12.09.2025;
accepted for publication: 01.10.2025