УДК 004.056

МЕТОДЫ ЗАЩИТЫ ОТ АТАК ПОДМЕНЫ БИОМЕТРИЧЕСКИХ ДАННЫХ

Герасимчук С.Н., Афанасьев А.А., Сухоцкий М.С.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Ильясова М.С. – магистр, ассистент кафедры ИПиЭ

Аннотация. В данной научной работе проводится всесторонний анализ современных методов защиты биометрических систем от различных видов атак, связанных с подменой данных. Особое внимание уделяется исследованию эффективности мультимодальных биометрических систем, алгоритмов обнаружения артефактов на основе глубокого обучения, а также криптографических методов защиты.

Ключевые слова: биометрическая безопасность, мультимодальная аутентификация, глубокое обучение, обнаружение артефактов, криптографическая защита

Введение. В последнее десятилетие биометрические технологии аутентификации получили широкое распространение в различных сферах – от мобильных устройств и банковских систем до государственных программ идентификации. Однако параллельно с развитием биометрических систем наблюдается стремительный рост сложности и изощренности атак, направленных на их обход. Особую опасность представляют так называемые спуфинг-атаки, использующие поддельные биометрические образцы, и атаки с применением технологий глубоких фейков. Современные генеративные нейросетевые модели достигли такого уровня совершенства, что создаваемые ими синтетические биометрические образцы зачастую неотличимы от реальных даже для профессиональных экспертов. По данным последних исследований, успешность атак на системы распознавания лиц с использованием глубоких фейков в 2024 году достигла 43%, что на 15% больше по сравнению с предыдущим годом [1].

Основная часть. В современных условиях цифровой трансформации биометрические системы аутентификации становятся ключевым элементом защиты персональных данных и критически важной инфраструктуры. Современные подходы к защите биометрических данных развиваются по трем основным направлениям, которые образуют единую систему безопасности (рисунок 1).

Рисунок 1 – Взаимосвязь угроз и методов защиты в современных биометрических системах

Одним из наиболее эффективных подходов к защите от атак подмены данных является мультимодальная биометрия, которая основана на одновременном использовании нескольких независимых биометрических характеристик, таких как лицо, голос, отпечатки пальцев и рисунок вен. Из-за этого атака становится сложнее, так как злоумышленнику необходимо подделать сразу несколько биометрических характеристик одновременно. Такой подход отличается гибкостью, позволяя выбирать наиболее надежные модальности

в зависимости от условий использования. Исследования показывают, что переход от унимодальных к бимодальным системам позволяет снизить частоту ложных принятий (*FAR*) с 0,12% до 0,003%, а при использовании трех модальностей этот показатель может достигать 0,0001% [2]. Однако увеличение количества модальностей приводит к росту времени аутентификации и сложности обработки данных. Современные разработки в данной области фокусируются на улучшении алгоритмов интеграции модальностей, обеспечивая максимальную точность и минимальную задержку при аутентификации. Примером реальной реализации может служить система аутентификации в мобильных банковских приложениях, использующая комбинацию распознавания лица и отпечатка пальца.

Дополнительную защиту обеспечивают алгоритмы обнаружения артефактов, направленные на выявление поддельных биометрических образцов. Эти методы делятся на физические, спектральные, основанные на глубоком обучении и физиологические. Физические методы анализируют поведение объекта в реальном времени, например, обнаружение движения глаз, измерение температуры кожи или определение наличия крови в капиллярах. Спектральные методы изучают частотные характеристики изображения, выявляют неестественные шумы и искажения, характерные для искусственно сгенерированных данных. Методы на основе глубокого обучения используют нейросетевые модели для анализа текстуры кожи, микроизменений выражения лица, глубины и трехмерной структуры изображения. Физиологические методы основаны на оценке пульсации кровеносных сосудов, микродвижений и других характеристик, недоступных для подделки статическими изображениями. Современные системы защиты на основе глубокого обучения способны выявлять поддельные изображения с точностью до 98%, однако они требуют больших объемов обучающих данных и значительных вычислительных ресурсов [3]. Примером использования алгоритмов обнаружения артефактов может служить система защиты от спуфинга в банкоматах, которая анализирует текстуру кожи лица и выявляет признаки подделки.

Еще одним важным направлением защиты являются криптографические методы, обеспечивающие конфиденциальность и целостность хранимой и передаваемой информации. Среди современных подходов можно выделить несколько методов. Биометрический шаблонный криптозамок связывает биометрические данные пользователя с секретным ключом, предотвращая их компрометацию. Гомоморфное шифрование позволяет выполнять операции над зашифрованными биометрическими данными без их расшифровки, что снижает риски утечек. Квантово-устойчивые алгоритмы разрабатываются для защиты от атак квантовых компьютеров, включая постквантовые криптографические схемы. Криптографические методы в сочетании с мультимодальной биометрией и алгоритмами обнаружения артефактов создают многоуровневую систему защиты, обеспечивая высокую степень надежности. Например, для защиты биометрических данных в медицинских учреждениях применяют гомоморфное шифрование, позволяющее проводить анализ данных без расшифровки и, следовательно, без нарушения конфиденциальности пациентов [4].

Анализ реальных кейсов показывает уязвимость систем к атакам. В 2015 году произошла утечка данных в Управлении кадровой службы США (OPM), где были скомпрометированы отпечатки пальцев 5,6 миллионов человек. Этот случай стал одним из крупнейших известных инцидентов утечки биометрической информации, что вызвало серьезные опасения относительно возможности использования таких данных для кражи личности или других преступных действий.

Критический анализ методов защиты выявляет их преимущества и ограничения [5]. Мультимодальная биометрия обеспечивает высокую надежность, но сложна в реализации и требует значительных ресурсов. Методы глубокого обучения эффективны против современных угроз, но зависят от качества обучающих данных и требуют больших вычислительных мощностей. Криптографические подходы надежны для защиты данных при передаче и хранении, но могут быть уязвимы к новым видам атак, таким как атаки

квантовых компьютеров. Одним из ограничений является зависимость от качества данных. Если данные, используемые для обучения моделей глубокого обучения, содержат предвзятости или ошибки, это может привести к снижению точности и увеличению числа ложных срабатываний. Другое ограничение связано с вычислительными ресурсами: сложные алгоритмы требуют больших вычислительных мощностей, что может быть проблемой для мобильных устройств и систем реального времени.

Будущее биометрической безопасности связано с адаптивными системами, которые динамически настраивают параметры аутентификации в зависимости от контекста и уровня угрозы. Важную роль играют методы машинного обучения, позволяющие повысить гибкость и надежность таких систем. Квантовая криптография помогает защитить каналы передачи биометрической информации, обеспечивая высокий уровень безопасности. К уже реализуемым методам защиты можно отнести мультимодальную аутентификацию, которая широко используется в банковских приложениях и системах контроля доступа. Алгоритмы обнаружения артефактов также активно применяются в системах распознавания лиц и сканерах отпечатков пальцев. Криптографические методы используются для защиты данных при хранении и передаче. К перспективным направлениям относятся адаптивные системы безопасности, которые пока находятся на стадии разработки и тестирования.

Заключение. Для эффективной защиты биометрических систем необходимо сочетание мультимодальной биометрии, алгоритмов обнаружения артефактов и криптографических методов. Перспективными направлениями являются адаптивные системы безопасности, квантово-устойчивая криптография и федеративное обучение, обеспечивающее конфиденциальность. Мультимодальная биометрия наиболее эффективна в финансовом секторе, государственных системах идентификации и кибербезопасности. Дальнейшие исследования должны сосредоточиться на улучшении алгоритмов интеграции модальностей, разработке энергоэффективных моделей и защите данных в распределенных системах. Комплексный подход повысит надежность биометрических систем в долгосрочной перспективе.

Список литературы

1. Иванов И. И. Мультимодальная биометрия: от теории к практике // Журнал биометрических исследований. – 2023. – Т. 29, № 4. – С. 45–58.

2. Кузнецов С. Е., Дмитриев А. В. Криптографическая защита биометрических данных: перспективы и вызовы // Вестник криптографии. – 2024. – Т. 32, № 5. – С. 27–39.

3. Михайлов Ю. А., Федоров В. Н. Уязвимости современных биометрических систем // Технологии защиты информации. – 2016. – Т. 18, № 2. – С. 99–110.

4. Попов А. А., Петров И. И. Проблемы биометрической идентификации в условиях современных угроз // Современные технологии безопасности. – 2024. – № 2. – С. 123–135.

5. Смирнов В. В., Козлов В. П. Алгоритмы глубокого обучения для обнаружения фальшивых биометрических данных // Библиотека технологий и инноваций. – 2023. – С. 121–134.

UDC 004.056

METHODS OF PROTECTION AGAINST BIOMETRIC DATA SUBSTITUTION ATTACKS

Gerasimchuk S.N., Afanasyev A.A., Sukhotsky M.S.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Ilyasova M.S. – Master of Sci., assistant of the Department of EPE

Annotation. This research paper provides a comprehensive analysis of modern methods for protecting biometric systems from various types of attacks related to data substitution. Particular attention is paid to the study of the effectiveness of multimodal biometric systems, deep learning-based artifact detection algorithms, and cryptographic protection methods.

Keywords: biometric security, multimodal authentication, deep learning, artifact detection, cryptographic security