УДК 004.056

УГРОЗЫ И УЯЗВИМОСТИ БИОМЕТРИЧЕСКИХ СИСТЕМ АУТЕНТИФИКАЦИИ: АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ СПУФИНГА

А. А. Лис

студент, Белорусский государственный университет, г. Минск, Беларусь, alisalis05@mail.ru

Научный руководитель **Н. И. Шандора**

старший преподаватель, Белорусский государственный университет, г. Минск, Беларусь, shandor@bsu.by

В данной научной работе проводится анализ угроз безопасности, связанных с использованием биометрических систем аутентификации, в контексте стремительного роста спуфинг-атак. Особое внимание уделяется исследованию эффективности различных способов обеспечения надежной защиты персональных данных. На основе анализа современных тенденций делается вывод о необходимости комплексного подхода.

Ключевые слова: биометрия; биометрические системы; спуфинг-атаки; мошенничество; токен; аутентификация.

THREATS AND VULNERABILITIES OF BIOMETRIC AUTHENTICATION SYSTEMS: ANALYSIS OF MODERN SPOOFING METHODS

A. A. Lis

student, Belarusian State University, Minsk, Belarus, alisalis05@mail.ru

Supervisor **N. I. Shandora**

senior lecturer, Belarusian State University, Minsk, Belarus, shandor@bsu.by

This scientific work provides a analysis of security threats associated with the use of biometric authentication systems, in the context of a rapid increase in spoofing attacks. Particular attention is paid to the study of the effectiveness of various methods for ensuring reliable protection of personal data. Based on an analysis of modern trends, the conclusion is made about the necessity of an integrated approach.

Keywords: biometrics; biometric systems; spoofing attacks; fraud; token; authentication.

Цифровизация играет ключевую роль и стремительно проникает во все сферы современного общества. В результате пользователи всё чаще сталкиваются с необходимостью идентификации себя. Одним из самых надёжных и популярных способов такой идентификации являются биометрические системы аутентификации. По прогнозам, к концу 2025 г мировой рынок биометрических систем достигнет 68,6 млрд долларов, что подчёркивает их растущую значимость [1]. Безопасность и защита биометрической информации играют важную роль при использовании биометрических систем. Биометрические данные, такие как отпечатки пальцев, лицо, голос и др., являются чрезвычайно чувствительной информацией, и их утечка может привести к серьезным последствиям. Однако, все более широкое использование биометрии привело к появлению многочисленных методов атак на биометрические системы. В настоящее

время такое явление как спуфинг стало одной из серьезных угроз в области цифровой безопасности.

Спуфинг (от англ. spoofing) – кибератака, при которой злоумышленник маскируется с целью хищения личной, финансовой, иной конфиденциальной информации, распространения вредоносного программного обеспечения [2].

Развитие искусственного интеллекта уменьшает сложность осуществления спуфинга и способствует росту числа атак. Согласно отчёту International Biometric Group (2024), число спуфинг-атак с 2020 г. выросло более чем на 3000 %. Наиболее уязвимыми оказались системы распознавания лиц (73 % случаев успешного обхода благодаря сгенерированным с помощью искусственного интеллекта дипфейкам), голосовая аутентификация (в 89 % случаев обман через синтетическое клонирование голоса), сканеры отпечатков пальцев (45 % успешных атак с использованием 3D-печатных реплик), сканирование радужки (23 % успеха при применении высококачественных фотографий) [3].

При использовании email-спуфинга злоумышленники подделывают настоящий адрес отправителя письма и создают видимость, что оно пришло от другого лица.

С помощью IP-спуфинга мошенники искажают IP-адреса в пакетах данных, которые передаются целевому серверу. Этот тип атак используется, чтобы скрыть истинное местонахождение злоумышленника в интернете.

DNS-спуфинг – тип спуфинга, предназначенный для подмена доменного имени с целью перенаправления пользователя на ложный сайт. Такие атаки нацелены на получение персональной информации или распространение вредоносных программ.

Для перехвата и подмены данных, передаваемых между двумя устройствами, злоумышленники используют ARP-спуфинг. С его помощью можно увидеть все пароли, а также конфиденциальную информацию, что делает небезопасной всю сеть.

С помощью Caller ID-спуфинг мошенники подменяют номера телефона. При входящем вызове на дисплее будет отображаться не тот номер, с которого на самом деле поступает звонок. На данный момент это является одной из самых распространенных методов спуфинга. Согласно недавнему опросу потребителей, более 70 % опрошенных заявили, что сталкивались с телефонными звонками, где собеседник выдавал себя за другое лицо. В то же время 74 % респондентов не отвечают на звонки с неизвестных номеров, опасаясь стать жертвами мошенничества. Кроме того, 70% опрошенных игнорировали звонки от реальных компаний, думая, что это мошенники, и лишь позже выясняли, что эти компании были настоящими [4].

Современные методы спуфинг-атак разнообразны и быстро развиваются. В результате этого, появляется все большая необходимость в использовании эффективных способов защиты информации.

Мультимодальные биометрические системы являются в настоящее время наиболее востребованными способами защиты от подмены данных, так как в своей работе используют не менее двух различных источников информации для идентификации личности (физиологический и поведенческий).

Идентификация по нескольким характеристикам предотвращает проблему спуфинга, так как она связана сразу с несколькими особенностями человека, поэтому злоумышленнику будет трудно подделать сразу несколько идентификаторов авторизованного пользователя.

Также, для биометрических систем одним из вариантов ее защиты является применение биометрической криптографии. При таком способе данные защищены с использованием системы симметричного шифрования, в то время как системы с открытым ключом используются для цифровых подписей и для безопасного обмена ключами между пользователями.

Существует несколько методов защиты ключей с использованием биометрии, одним из которых является удаленное сопоставление шаблонов и хранение ключей. В этом подходе биометрическое изображение пользователя захватывается и сравнивается с хранящимся шаблоном, после успешной верификации ключ высвобождается из безопасного хранилища.

Еще один способ защиты биометрических данных – аппаратные токены. Для этого требуется устройство, которое владелец носит с собой для получения разрешения на доступ к сетевым ресурсам. Каждый токен имеет уникальный секретный криптографический ключ, хранящийся внутри него, используемый для установления личности токена.

Сторона, устанавливающая аутентификацию, отправляет запрос, ответ на который вычисляется с использованием секретного ключа. Секретный ключ никогда не должен покидать токен. Попытки взломать токен, чтобы восстановить ключ, должны привести к уничтожению ключа.

Аутентификация на основе токенов сегодня является технической реальностью, но ей все еще не пользуется большой популярностью. Многие существующие системы используют настольную рабочую станцию в качестве «токена» для аутентификации с остальной частью сети. Криптографический ключ вычисляется рабочей станцией на основе пароля пользователя, на основе которой рабочая станция аутентифицирует в сети.

Биометрические системы аутентификации становятся неотъемлемой частью цифрового мира, обеспечивая удобство и высокую точность идентификации. Вместе с тем они остаются уязвимыми к разнообразным спуфинг-атакам – от подмены сообщений и GPS-координат до атак на лицо, голос, отпечатки пальцев и радужку. Рост числа таких атак, стимулируемый развитием технологий искусственного интеллекта, подчёркивает необходимость комплексной защиты. Наиболее эффективными мерами остаются мультимодальные системы, биометрическая криптография и аппаратные токены, которые обеспечивают надёжную верификацию и безопасное хранение данных. Только сочетание современных технологий, безопасного механизма и информирования пользователей позволяет минимизировать риски и сохранить доверие к биометрической аутентификации.

Библиографические ссылки

1. Biometric technologies – statistics & Facts. URL: https://www.statista.com/topics/4989/biometric-technologies/?srsltid=AfmBOop3Q-ABAyRZMyoTPRLunHmVgb4h1tfdWMPcIljh7nN_nfoootms (date of access: 22.09.2025).

2. Энциклопедия Касперского / Спуфинг (spoofing). URL: https://encyclopedia.kaspersky.ru/ glossary/spoofing (дата обращения: 22.09.2025).

3. Biometric Spoofing: How Deep Fakes Fool Identity Systems. URL: https://www.carmel.so/stories/biometric-spoofing (date of access: 22.09.2025).

4. Nearly 80 % of Consumers Consider Phone Channel Important for Communicating with Businesses, Despite Reluctance to Answer Calls. URL: https://newsroom.transunion.com/nearly-80-of-consumers-consider-phone-channel-important-for-communicating-with-businesses-despite-reluctance-to-answer-calls (date of access: 22.09.2025).