ISSN 2181-3187

СРАВНИТЕЛЬНАЯ АНАЛИЗ УГРОЗЫ И АТАКИ НА БИОМЕТРИЧЕСКУЮ АУТЕНТИФИКАЦИЮ

Бозоров Сухробжон Мумин ўғли

Старший преподаватель кафедры Криптологии,

Ташкентский университет информационных технологий имени Муҳаммад ал-Хоразмий

Аннотация

В статье представлен сравнительный анализ угроз и атак на биометрическую аутентификацию в условиях роста киберугроз и цифровизации. Рассматриваются традиционные методы аутентификации (пароли, токены) и их ограничения в сравнении с биометрическими подходами, которые обеспечивают высокий уровень безопасности и удобства за счёт анализа уникальных физиологических и поведенческих характеристик. Описаны основные векторы атак на биометрические системы, включая презентационные атаки (spoofing), искажение процесса извлечения признаков и компрометацию баз шаблонов. Особое внимание уделено атакам с использованием технологий deepfake и генеративных состязательных сетей (GAN). Предложены методы противодействия, такие как обнаружение живости (liveness detection), шифрование данных и многофакторная аутентификация. Результаты подчёркивают необходимость разработки устойчивых алгоритмов и комплексных защитных стратегий для обеспечения надёжности биометрических систем.

Ключевые слова: Биометрическая аутентификация, информационная безопасность, киберугрозы, презентационные атаки, deepfake, генеративные сети, liveness detection, распознавание лиц, шифрование данных, многофакторная аутентификация, атаки на биометрические шаблоны, враждебные атаки, машинное обучение.

ISSN 2181-3187

Введения

Аутентификация представляет собой фундаментальный процесс подтверждения подлинности личности пользователя, необходимый для обеспечения информационной безопасности и предотвращения несанкционированного доступа к защищенным системам.

В современных условиях стремительного развития цифровых технологий традиционные методы аутентификации, основанные на использовании паролей и PIN - кодов, демонстрируют снижение эффективности и уязвимость перед современными угрозами.

Существуют три основных класса методов аутентификации:

– знание (что знает пользователь): пароли, PIN - коды;

– владение (Что имеет сам пользователь): смарт-карты, токены, USB - ключи;

– биометрия (Кем он/она является): отпечаток пальца, распознавание лица, характеристику информацию о самом владельце физиологию.

Анализ современных методов аутентификации показывает необходимость перехода от традиционных подходов к более надежным решениям. В условиях растущих кибер-угроз особую значимость приобретают биометрические методы, сочетающие высокий уровень безопасности с удобством использования. Рассмотрим особенности каждого метода:

Парольная аутентификация

Наиболее широко распространённым методом подтверждения личности является парольная аутентификация. Её суть заключается в предоставлении пользователем заранее известной секретной информации — пароля — для прохождения процедуры идентификации.

Аутентификация на основе токенов

ISSN 2181-3187

Данный метод базируется на владении физическим или программным устройством, генерирующим одноразовые коды или криптографические подписи. В зависимости от реализации токены делятся на аппаратные и программные. Аппаратным токенам относятся физические устройства (например, смарт-карты, USB - ключи типа YubiKey). Они обеспечивают высокий уровень безопасности, так как мало подвержены программным атакам.

Программные токены: используются в виде мобильных приложений, таких как Google Authenticator или Microsoft Authenticator. Они генерируют одноразовые пароли, действительные в течение ограниченного времени. Уязвимы к вредоносному ПО и компрометации мобильных устройств.

Биометрическая аутентификация

Биометрические методы базируются на анализе уникальных физиологических и поведенческих характеристик человека. Они демонстрируют высокую точность и удобство в применении, особенно в условиях частого доступа. Наиболее перспективным направлением считается биометрическая аутентификация, поскольку она основывается на уникальную физиологию или поведенческих характеристиках человека. Это позволяет обеспечить более высокий уровень безопасности и удобства по сравнению с традиционными методами [1].

Таблица 1

Сравнение биометрической аутентификации с другими методами

Тип аутентификации	**Безопасность**	**Удобство**	**Риск компрометации**
Биометрическая аутентификация	Высокая	Отличное	Минимальный
Пароли/PIN - коды	Средняя в зависимости от	Низкое (требуется	Высокий

ISSN 2181-3187

	пароля	запоминать)	
Аутентификация на основе токенов	Средняя (можно украсть)	Низкое требуется носить собой	Средняя

Как следует из сравнения, каждый метод аутентификации обладает собственными преимуществами и ограничениями. Так, пароли отличаются простотой внедрения и низкими затратами, однако подвержены рискам подбора, фишинга и социальной инженерии. Напротив, биометрические системы обеспечивают высокий уровень надёжности за счёт использования уникальных физиологических или поведенческих признаков, но требуют значительных инвестиций в разработку, оборудование и сопровождение.

Биометрическая идентификация опирается на анализ устойчивых и трудноизменяемых биологических характеристик, что значительно снижает риски подмены личности и несанкционированного доступа. Интеграция биометрических технологий в системы контроля и управления доступом (СКУД) обеспечивает эффективную защиту критически важных объектов, информационных ресурсов и материальных ценностей.

Таблица 2

Сравнение биометрических методов аутентификации

Название	**Точность**	**Стоимость**	**Описание**
Отпечаток пальца	77%	Низкая (500-2000 долларов)	Используется для анализа уникальных линий на пальцах.
Лицо	97,53%	Средняя (1-5 тысяч долларов)	Распознает уникальные черты лица: форму глаз, носа, подбородка и другие

ISSN 2181-3187

Голос	90-95%	Низкая (500- 3.000 долларов)	Анализирует уникальные характеристики речи: тон, тембр, акцент и скорость.
Сетчатка глаза	~99.9%	Высокая (5 -20 тысяч долларов)	Использует уникальные кровеносные сосуды сетчатки, которые не меняются в течение жизни.
Походка	До 94%	Выше среднего (3 -10 тысяч долларов)	Анализирует параметры походки: длина шага, симметрия, скорость и другие.

Угрозы и атаки на биометрическую аутентификацию

В настоящее время вопрос обеспечения безопасности биометрических систем приобретает особую актуальность в контексте растущей цифровизации общества. Таким образом, исследование угроз и атак на биометрическую аутентификацию становится важнейшей задачей для обеспечения надежности и безопасности современных информационных систем.

Необходимость анализа существующих уязвимостей и разработки методов противодействия обуславливает значимость данного направления научных исследований.

Классификация атак по этапам обработки данных

Атаки на биометрические системы можно классифицировать по следующим критериям:

1. Атаки на устройство ввода

Устройство ввода (камера или инфракрасный сенсор) захватывает изображение лица пользователя — первая точка взаимодействия, наиболее уязвимая к внешним воздействиям. Злоумышленник может вмешаться именно на этом этапе, подставив поддельные данные: фотографию, видео, дипфейк или

ISSN 2181-3187

3D - маску (презентационная атака, spoofing). Этот этап является первой точкой взаимодействия и наиболее подвержен атакам, так как злоумышленники могут напрямую манипулировать входными данными.

Презентационные атаки (Spoofing) — предоставление поддельных данных (фотографии, видеозаписи, дипфейки, 3D - маски).

Рис 1. Иллюстрация подделки лица.

Атака на устройство ввода позволяет обойти биометрическую систему и получить несанкционированный доступ к оборудованию, учётной записи или защищённым данным. Мотивами подобных действий могут быть кража персональной и финансовой информации, коммерческий или политический шпионаж, а также другие преступные цели.

Одним из распространённых способов обхода биометрических систем является демонстрация сгенерированного или заранее записанного дипфейк-видеоматериала. Система, не оснащённая надёжным механизмом проверки «живости», воспринимает такую подделку как реальное лицо пользователя. Для противодействия этим угрозам внедряются методы liveness detection —

ISSN 2181-3187

определения присутствия живого объекта. Эти методы включают, в частности, анализ реакции зрачков на изменение освещения, отслеживание микродвижений мышц лица, а также регистрацию теплового излучения, присущего живому человек. [1].

2. Атаки на параметризацию сигнала

Данный тип атак направлен на искажение процесса извлечения биометрических признаков, что непосредственно влияет на этап последующего сравнения шаблонов. Атака реализуется путём внесения малозаметных, зачастую невидимых для человеческого глаза искажений в изображение лица. Эти искажения оказывают влияние на работу нейронной сети, приводя к формированию некорректного биометрического шаблона. В результате может возникнуть ложная идентификация пользователя либо отказ в доступе легитимному субъекту аутентификации.

Основной целью является создание искажённого шаблона признаков, который нарушает корректную работу системы распознавания, провоцируя ошибочную идентификацию — как в сторону предоставления доступа злоумышленнику, так и в виде отказа в доступе действующему пользователю. Для повышения устойчивости биометрических систем к подобным атакам применяются следующие меры: использование устойчивых архитектур глубокого обучения, включающих защитные слои и методы регуляризации, мониторинг и анализ входных данных на предмет аномалий и предварительная фильтрация обучающих выборок с целью исключения потенциально вредоносных или искусственно модифицированных данных.

3. Атаки на базу шаблонов

Атаки направлены на хранилище биометрических данных, где содержатся шаблоны (векторы признаков), полученные в результате обработки биометрической информации пользователя. Поскольку компрометация

ISSN 2181-3187

биометрических шаблонов может иметь необратимые последствия. В отличие от паролей, биометрические характеристики невозможно изменить, что делает их особенно уязвимыми при утечке.

Целью является нарушение конфиденциальности биометрических данных, а также возможность последующего использования скомпрометированных шаблонов для получения несанкционированного доступа к системам, сервисам или устройствам [2].

Учитывая чувствительность биометрических данных и невозможность их восстановления в случае компрометации, обеспечение их безопасности требует комплексного подхода.

В современных системах применяются следующие методы защиты биометрических шаблонов:

– шифрование данных с использованием криптографических алгоритмов высокой стойкости обеспечивает защиту шаблонов как при хранении, так и при передаче по сетям;

– внедрение аппаратных модулей безопасности позволяет изолировать биометрические шаблоны в защищённых аппаратных средах, что значительно снижает риск их кражи;

– разделение биометрических шаблонов и распределение их между несколькими физическими логическими хранилищами минимизирует вероятность компрометации данных в случае взлома одного из узлов;

– регулярное проведение аудита, ведение журналов активности и реализация принципа минимальных прав позволяют контролировать.

ISSN 2181-3187

Рис 2. Все процессы при атаке на биометрическую аутентификацию

Классификация по характеру воздействия

Рис 3. Классификация типов кибератак и соответствующих контрмер

Пассивные атаки направлены на использование изображений или видео, полученных без ведома владельца. Злоумышленники могут извлекать данные о лице из публичных источников, таких как социальные сети или камеры наблюдения. В некоторых случаях применяются изображения высокого качества

ISSN 2181-3187

или 3D - модели лиц, что позволяет системе ошибочно идентифицировать чужое лицо как настоящее. Такие атаки не требуют активного вмешательства в работу системы и могут быть эффективны, если система не защищена от подобных угроз.

Активные атаки предполагают непосредственное вмешательство злоумышленника в процесс распознавания. Одним из распространённых методов является использование масок или 3D - моделей лиц, изготовленных с помощью современных технологий. Также используются видео-анимированные изображения или deepfake - видео, которые создают иллюзию реального лица и могут привести к ошибочному распознаванию.

Атаки на системы распознавания лиц и методы защиты

В условиях стремительного развития технологий искусственного интеллекта (ИИ) и машинного обучения злоумышленники получают доступ к новым методам атак, которые значительно усложняют защиту биометрических систем.

Анализ передовых технологий показывает, что современные угрозы сосредоточены на использовании достижений ИИ для создания синтетических данных и манипуляции существующими моделями. Рассмотрим три ключевых вектора атак: Deepfake - технологии, генеративные модели и атаки.

1. Deepfake - технологии

Deepfake - технологии основаны на генеративно-состязательных сетях (GAN), которые способны создавать синтетические изображения и видео высокой реалистичности. Основная задача сымитировать поведение и внешний вид легитимного пользователя для обхода систем биометрической аутентификации. Целью атак с помощью deepfake:

ISSN 2181-3187

– получение привилегий или ресурсов защищённой системы через ложную идентификацию образом легитимного пользователя.

– тестирование и сбор данных о реакции системы на продвинутые попытки обхода, выявления уязвимости и оптимизировать дальнейшие атаки.

– провоцирование ложных срабатываний как положительных, так и отрицательных с целью подрыва доверия к биометрическому решению и создания репутационных рисков для разработчика или оператора системы [4].

Рисунок 4. Схема реализации deepfake

Сбор исходных данных - фотографий, видеозаписей и аудиофрагментов целевого пользователя с открытых источников. Создание deepfake на собранном датасете для синтеза «живая» видеозаписи пользователя. Разработка сценария внедрения поддельного видео: выбор точки входа, проработка таймингов и оценка рисков. Обнаружение попытки атаки (срабатывание механизмов «liveness detection», записи логов).

2. Генеративные состязательные сети (GAN) позволяют создавать высокореалистичные синтетические биометрические образцы — в данном случае «лиц», практически неотличимые от фотографий живых людей.

ISSN 2181-3187

Рисунок 5. Пример генерации искусственного лица

Атака реализуется в несколько этапов в начале генератор учится преобразовывать случайный вектор (шум) в изображение лица, подгоняя его под статистику целевого датасета. После сходимости модели генерируются изображения или видеоролики, где «лицо» целевого пользователя демонстрирует естественные микродвижения. Сгенерированное изображение предъявляется системе распознавания лица биометрический алгоритм не различает фейк от реального пользователя, происходит ложная авторизация и злоумышленник получает доступ к защищённой зоне или сервису.

3. Враждебные атаки направлены на манипуляцию входными данными с целью обмана моделей машинного обучения. Злоумышленник вносит в изображения микроскопические, часто незаметные для человеческого глаза искажения, которые нарушают работу нейронной сети на этапе извлечения признаков. В результате применения таких искажений модель формирует неверный биометрический шаблон — это может привести как к ложным положительным срабатываниям пропуск злоумышленника, так и к ложным отрицательным [3].

ISSN 2181-3187

Модифицированные изображения используются для обхода системы распознавания лиц или для создания хаоса в работе алгоритмов. На практике это может выглядеть как злоумышленник демонстрирует системе изображение своего лица либо удалённо подменяет видеопоток, что приводит к прямому обходу защиты.

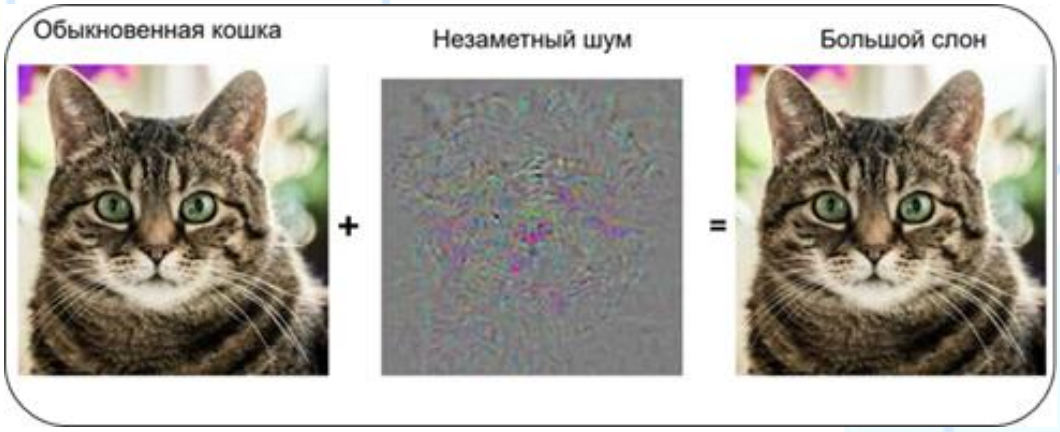

Рис 6. Пример реализация враждебной атаки

Целью враждебных атак является снижение точности работы системы распознавания лиц или создание ложных положительных результатов.

Таблица 3

Методы противодействия к различным атакам

Метод противодействия	Описание
Обнаружение живости (Liveness Detection)	Использование алгоритмов для определения, что объект на изображении — это реальное лицо, а не фотография или видео. Методы включают анализ движений глаз, рта или моргания.
Использование глубокой нейронной сети для обнаружения фальсификаций	Обучение моделей для выявления поддельных изображений или видео, сгенерированных с помощью технологий.

ISSN 2181-3187

3D - распознавание лиц	Использование технологий 3D - сканирования для повышения точности и защиты от атак с использованием плоских 2D - изображений.
Инфракрасная проверка	Использование инфракрасных датчиков для анализа теплового профиля лица. Живой организм имеет характерную тепловую карту, которую сложно подделать, что повышает уровень защиты системы.
Анализ движения и выражений лица	Внедрение алгоритмов, которые отслеживают и анализируют выражения и движения лица для предотвращения использование статичных изображений или видео.

Эта таблица наглядно отображает методы противодействия атакам на системы распознавания лиц.

Анализ современных векторов атак демонстрирует, что злоумышленники активно используют достижения искусственного интеллекта для обхода систем распознавания лиц. Для минимизации рисков необходимо внедрять комплексные меры защиты, включающие алгоритмы детекции живости, шифрование данных и многофакторную аутентификацию. Только сочетание этих подходов способно обеспечить эффективную защиту биометрических систем от современных и перспективных угроз [3].

Особое внимание уделяется угрозам, направленным на искажение процесса извлечения признаков, что может привести к ошибочным результатам распознавания и снижению надежности системы. Применяемые атаки, такие как добавление незаметных для человеческого глаза искажений, создающих ложные шаблоны, или использование поддельных биометрических данных, наглядно подчёркивают необходимость защиты биометрических систем от внешних вмешательств.

ISSN 2181-3187

Системы биометрической аутентификации требуют применения более устойчивых механизмов защиты, включающих разработку алгоритмов, способных противостоять множеству атак, а также постоянный мониторинг биометрических данных на предмет аномалий. В условиях эволюции векторов атак ключевым фактором безопасности остаётся динамичное совершенствование технологий распознавания лиц и оперативное обновление защитных стратегий.

Устойчивость биометрических систем напрямую зависит от их способности адаптироваться к новым видам атак. Для этого необходимо: – постоянно совершенствовать алгоритмы защиты; – разрабатывать интеллектуальные методы детекции внешних воздействий; – внедрять гибкие и адаптивные механизмы реагирования.

Исследование угроз и атак на биометрическую аутентификацию подчёркивает необходимость постоянного развития защитных механизмов и создания новых стратегий противодействия. В дальнейшем следует уделять особое внимание разработке алгоритмов, устойчивых как к современным, так и к перспективным атакам, а также развитию комплексных подходов к защите.

Заключения

Исследование выявило, что биометрические системы аутентификации обеспечивают высокий уровень безопасности и удобства по сравнению с традиционными методами, основанными на паролях и токенах, однако они подвержены сложным атакам, включая презентационные атаки, манипуляции с извлечением признаков и компрометацию баз шаблонов. Современные угрозы, такие как deepfake и генеративные состязательные сети, требуют внедрения передовых методов защиты, включая алгоритмы обнаружения живости, инфракрасную проверку и шифрование данных. Для повышения устойчивости биометрических систем необходимы комплексные подходы, сочетающие

ISSN 2181-3187

многофакторную аутентификацию, мониторинг аномалий и регулярное обновление защитных механизмов. Дальнейшие исследования должны быть направлены на разработку адаптивных алгоритмов, способных противостоять эволюционирующим киберугрозам, и интеграцию интеллектуальных методов анализа для обеспечения надёжности и доверия к биометрическим технологиям в условиях стремительного развития искусственного интеллекта.

Список использованных литературы

1. Chingovska, I., Anjos, A., & Marcel, S. On the Effectiveness of Local Binary Patterns in Face Anti-Spoofing. BIOSIG, 2012.
2. Источник: Bowyer, K. W., Chang, K., & Flynn, P. A Survey of Approaches and Challenges in 3D and Multi-modal 3D+2D Face Recognition. 2006.
3. Turk, M. A. & Pentland, A. P. «Eigenfaces for Recognition». Journal of Cognitive Neuroscience, 3(1), 71–86, 1991.
4. Belhumeur, Y. N., Hespanha, J. P. & Kriegman, D. J. «Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection». IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7), 711–720, 1997.