УДК 004.056.53

С.С. Волкова
Вологодский государственный университет

АНАЛИЗ УЯЗВИМОСТЕЙ ЛИЦЕВЫХ БИОМЕТРИЧЕСКИХ СИСТЕМ

Статья посвящена анализу уязвимостей систем биометрической аутентификации пользователей информационных систем по изображению лица. Приведена классификация атак, а также определены меры противодействия различным типам атак.

Аутентификация, лицевая биометрия, несанкционированный доступ, атака спуфинга.

Современные системы аутентификации сложно представить без биометрических технологий. Такие системы могут использоваться для доступа в образовательные учреждения, при подтверждении электронных платежей, а также для доступа к интернет-банкингу.

Рядом биометрических компаний и исследовательских институтов разработаны системы биометрической аутентификации, использующие различные модальности: лицо, отпечаток пальца, сетчатку глаза, голос. Однако в результате их внедрения был выявлен ряд проблем, связанных с защищенностью от угроз безопасности системы.

Угрозы безопасности системы можно условно разделить на следующие типы [1]: угрозы нарушения целостности информации, угрозы нарушения конфиденциальности информации и угрозы нарушения работоспособности системы. В случае реализации угрозы нарушения целостности информации она может быть искажена или изменена, что может привести к нарушению качества информации или полному ее уничтожению. Угрозы нарушения конфиденциальности информации направлены на получение доступа лицам, доступ которым для нее закрыт или ограничен. Угрозы нарушения работоспособности системы ориентированы на снижение работоспособности информационной системы либо на блокировку доступа к некоторым ее ресурсам.

На основании методического документа, утвержденного ФСТЭК РФ 11 февраля 2014 г. [2], угрозы безопасности информации определяются по результатам оценки потенциала, оснащенности и мотивации внутренних и внешних нарушителей, анализа возможных уязвимостей системы, потенциальных способов реализации угроз безопасности информации и последствий от нарушения признаков безопасности информации (целостности, конфиденциальности, доступности).

Качество проводимых мероприятий, принимаемых для защиты информации в информационной системе, зависит от эффективности определения угроз безопасности информации для определенной информационной системы в определенных условиях ее функционирования.

Выбираемые для реализации в системе меры защиты информации должны гарантировать блокировку одной или нескольких угроз безопасности информации, включенных в модель угроз безопасности информационной системы.

Нарушения целостности и конфиденциальности информации в целом, а также доступности и целостности отдельных компонентов информационной системы могут быть вызваны многообразными нарушениями. Одним из наиболее распространенных нарушений является несанкционированный доступ [3]. Угроза несанкционированного доступа на текущий момент несет одну из основных опасностей для безопасности информационной системы, т.к. злоумышленник может выполнить незаконное проникновение в информационную систему и получить возможность к реализации вышеприведенных угроз. Основной целью несанкционированного доступа является получение нарушителем доступа к системе в обход установленных в соответствии с принятой политикой безопасности правил разграничения доступа.

Из всех известных способов получения несанкционированного доступа следует обратить внимание на следующие наиболее распространенные: перехват аутентификационной информации, «маскарад», незаконное использование привилегий [3].

Перехват аутентификационной информации осуществляется с использованием специального программного обеспечения. Чаще всего программа-перехватчик имитирует прием аутентификационной информации таким образом, что пользователь самостоятельно передает ее злоумышленнику, полагая, что работает с реальной системой.

Для «маскарада» характерно присвоение полномочий и привилегий другого пользователя либо вменение каких-либо действий другому пользователю. Например, «маскарадом» является передача сообщений от имени другого пользователя. Особенно опасно такое нарушение в системах электронных платежей, когда неверная аутентификация клиента может привести к большим убыткам для него.

При несанкционированном захвате привилегий злоумышленник может получить возможность выполнения определенных действий внутри системы, обходя систему защиты. Часто возможность осуществления такого способа появляется из-за халатности администратора при назначении привилегий либо при наличии ошибок в системе защиты.

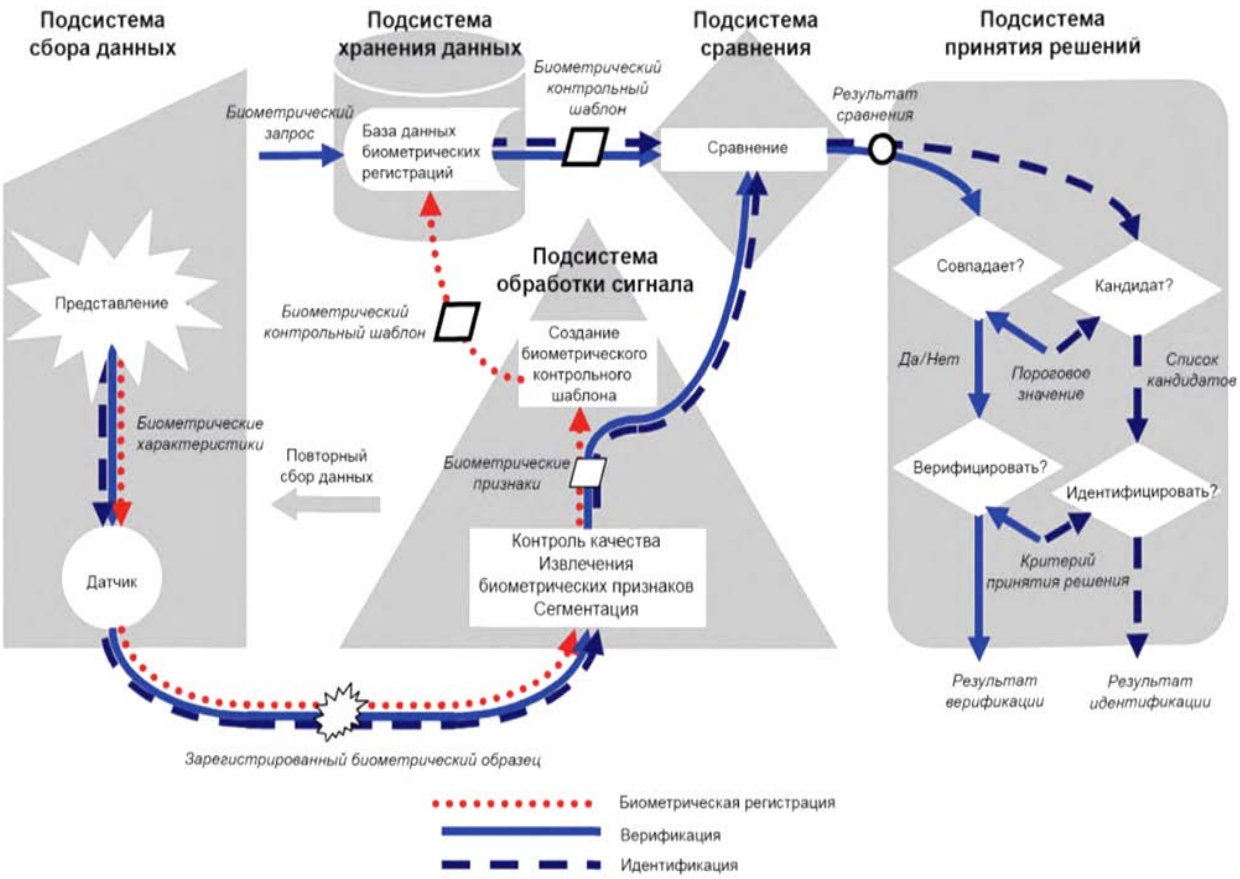

Рис. Компоненты биометрической системы общего вида

Каждый из этих способов получения несанкционированного доступа направлен на отдельные подсистемы информационной системы. Биометрическая информационная система состоит из подсистемы сбора данных, подсистемы хранений данных, подсистемы сравнения и подсистемы принятия решений. Обобщенная схема биометрической аутентификации показана на рисунке [4].

На каждый из этих компонентов могут быть осуществлены различные виды атак: атаки на канал связи, на базу данных, на захват данных, их обработку и принятие решения.

За исключением атаки на устройство ввода, все перечисленные атаки не относятся конкретно к лицевым биометрическим системам и являются общими для различных модальностей. Противодействие таким атакам осуществляется шифрованием канала передачи данных и применением цифрового кодирования. Атаки же на модуль ввода биометрической информации отличаются для различных модальностей, при этом этот компонент системы остается наиболее уязвимым, поскольку он подвержен атаке спуфинга [5] – попытке подмены биометрической характеристики путем представления сенсору поддельного объекта идентификации.

В лицевых биометрических системах неавторизованные клиенты (злоумышленники) могут произвести попытку обмана системы подменой изображения лица авторизованного пользователя видеоизображением его лица или просто его фотографией. В настоящее время исследователи фокусируются на вопросе противодействия таким атакам [6, 7], однако они по-прежнему достаточно успешны.

Устойчивость систем лицевой биометрической аутентификации к спуфинг-атакам – одна из первостепенных задач для противодействия несанкционированному доступу к информационной системе.

При атаке спуфинга на лицевую биометрическую систему объект идентификации может быть подделан с использованием распечатанной фотографии, видеозаписи, показанной на экране монитора или мобильного телефона, а также с использованием трехмерной модели головы пользователя [8].

Самая дешевая и простая для реализации атака – атака с использованием распечатанной фотографии. При этом для имитации поведения человека злоумышленник может выполнить изгиб или поворот фотографии. Более серьезной угрозой является атака с использованием видеозаписи, т.к. имитация поведения человека осуществляется более реалистично. Трехмерная модель головы имеет больше пространственной информации о пользователе, однако при данном способе атаки сокращается количество физиологической информации о лице пользователя. Кроме того, трудно создать реалистичную трехмерную модель живого человека без его участия. Таким образом, наиболее распространенными способами подделки аутентификационной информации в лицевых биометрических системах остаются использование фотографии и видеозаписи человека.

Противодействие атаке спуфинга можно осуществлять как с помощью дополнительных датчиков, так и без них, используя только основной сенсор. Методы с использованием трехмерных сканеров и дополнительных датчиков [9–11] показывают высокую эффективность, однако их применение затруднено необходимостью использования специального оборудования.

Поэтому методы, использующие только основной сенсор биометрической системы, являются более предпочтительными, т.к. обладают свойством легкой интеграции в существующую систему, которая как правило оборудована только камерой. Для определения подделки в методах, не использующих специального оборудования, чаще всего анализируются характеристики действий пользователя, особенности движения трехмерных объектов, а также текстурные признаки [12].

Характеристики действий пользователя могут как требовать обратную связь от пользователя (например, улыбнуться или подмигнуть), так и не требовать конкретной активности пользователя, базируясь на независимых от внешних указаний действиях (например, регулярное моргание) [13, 14]. При этом анализ данных характеристик показывает высокое качество для атак с использованием фотографии или трехмерной модели головы пользователя. Однако данный подход в значительной степени зависит от определения контрольных точек лица и может дать большое число ложноотрицательных ответов.

При анализе особенностей движения трехмерных объектов основываются на том, что фотография как плоский объект генерирует иные паттерны движения, в отличие от трехмерного человеческого лица [15, 16]. Такой подход показывает высокое качество, но только в тех случаях, когда информации о движении достаточно, – ошибки могут возникать, например, при анализе изображений низкого качества.

Кроме того, методы, основывающиеся на анализе движения и действия, могут быть неэффективны при использовании видеозаписи пользователя информационной системы.

Анализ текстурных признаков направлен на выделение особенностей, не характерных для «живого» человека. Такие особенности могут возникать в процессе печати, их может генерировать структура бумаги и экран, на котором производится отображение, что позволяет отличить поддельное изображение от реального лица [17–19]. При этом такой подход не требует обратной связи от пользователя и прост в реализации.

Однако обнаружение таких особенностей может быть затруднено в некоторых случаях. Например, развитие дисплеев высокой четкости может привести к трудности в различении текстур реального человека и подделки за счет увеличения качества воспроизведения интенсивности цветов.

Следовательно, при разработке методов противодействия спуфинг-атакам на лицевую биометрическую систему следует более пристально обращать внимание на схему спуфинга, источником которого является воспроизведенная на экране с высоким разрешением видеозапись человеческого лица.

Таким образом, в данной работе описаны угрозы безопасности лицевой биометрической информационной системы. Показано, что устойчивость биометрической системы аутентификации пользователя по изображению лица к спуфинг-атаке (попытке подмены биометрической характеристики) является одной из основных задач для предотвращения несанкционированного доступа к информационной системе. Приведены примеры атак на считыватель биометрической информации, а также показаны способы противодействия такого типа атакам.

Литература

1. Зегежда, Д. П. Как построить защищенную информационную систему / Д. П. Зегежда, А. М. Ивашко ; под ред. Д. П. Зегежды и В. В. Платонова. – Санкт-Петербург : Мир и семья, 1997. – 312 с.
2. Меры защиты информации в государственных информационных системах : методический документ ФСТЭК от 11 февраля 2014 г. – URL: http://fstec.ru/component/attachments/download/675. – Текст : электронный (дата обращения: 26.10.2021).
3. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – Москва : Радио и связь, 2001. – 376 с.
4. ГОСТ ISO/IEC 19794-1-2015. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура. – URL: http://docs.cntd.ru/document/1200129505. – Текст : электронный (дата обращения: 26.10.2021).
5. Matsumoto, T. Impact of Artificial ”Gummy” Fingers on Fingerprint Systems / Matsumoto, T. // Optical Security and Counterfeit. – 2002. – Vol. 4677, № IV. – P. 275–289.
6. A Survey on Anti-Spoofing Methods for Facial Recognition with RGB Cameras of Generic Consumer Devices / Z. Ming, M. Visani, M. M. Luqman, J. C. Burie // Journal of Imaging. – 2020. – Т. 6, №. 12. – P. 139.
7. Raheem, E. A. Insight on face liveness detection: A systematic literature review / E. A. Raheem, S. M. S. Ahmad, W. A. W. Adnan // International Journal of Electrical & Computer Engineering (2088-8708). – 2019. – Т. 9, № 6.
8. Pan, G. Liveness detection for face recognition / G. Pan, Z. Wu, L. Sun // INTECH Open Access Publisher. – 2008. – P. 109–124.
9. Liveness detection based on 3D face shape analysis / A. Lagorio, M. Tisterelli, M. Cadoni et al. // Biometrics and Forensics (IWBF) 2013 International Workshop on. – 2013. – P. 1–4.
10. Albakri, G. The effectiveness of depth data in liveness face authentication using 3D sensor cameras / G. Albakri, S. Alghowinem // Sensors. – 2019. – Т. 19, №. 8. – P. 1928.
11. Костылев, Н. М. Модуль определения витальности лица по спектральным характеристикам отражения кожи человека / Н. М. Костылев, А. В. Горевой // Инженерный журнал: наука и инновации. – 2013. – № 9 (21). – С. 47.
12. Chakarborty, S. An overview of face liveness detection / S. Chakarborty, D. Das // In International Journal on Information Theory. – 2014. – №. 3 (2). – P. 11–25.

13. Jee, Hyung-Keun. Liveness Detection for Embedded Face Recognition System / Hyung-Keun Jee, Sung-Uk Jung, Jang-Hee Yoo // Proceedings of World Academy of Science, Engineering and Technology. – 2006. – Vol. 18. – P. 29–32.

14. Singh, A. K. Face recognition with liveness detection using eye and mouth movement / A. K. Singh, P. Joshi, G. C. Nandi // 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014). – IEEE, 2014. – P. 592–597.

15. Bao, W. A liveness detection method for face recognition based on optical flow field / W. Bao, H. Li, W. Jiang // In. Proceedings of the 2009 International Conference of Image Analysis and Signal Processing, Tiazhou, China. – P. 233–236.

16. Yin, W. A face anti-spoofing method based on optical flow field / W. Yin, Y. Ming L. Tian // 2016 IEEE 13th International Conference on Signal Processing (ICSP). – IEEE, 2016. – P. 1333–1337.

17. Face liveness detection: fusing colour texture feature and deep feature / F. M. Chen, C. Wen, K. Xie et al. // IET Biometrics. – 2019. – Т. 8. – №. 6. – P. 369–377.

18. Kavitha, P. Fuzzy local ternary pattern and skin texture properties based countermeasure against face spoofing in biometric systems / P. Kavitha, K. Vijaya // Computational Intelligence. – 2021. – Т. 37, №. 1. – P. 559–577.

19. Волкова, С. С. Применение сверточных нейронных сетей для решения задачи противодействия атаке спуфинга в системах лицевой биометрии / С. С. Волкова, Ю. Н. Матвеев Ю. Н. // Научно-технический вестник информационных технологий, механики и оптики. – 2017. – Т. 17, № 4. – С. 702–710.

S.S. Volkova
Vologda State University

VULNERABILITY ANALYSIS OF FACIAL BIOMETRIC SYSTEMS

The article is devoted to vulnerability analysis of facial authentication systems. A hierarchy of attack is provided and countermeasures techniques for different types of attacks are defined.

Authentication, facial biometric system, unauthorized access, spoofing-attack.