УДК 004

«Свой» или «Чужой»: влияние уязвимостей на работоспособность биометрических систем

Комарова Ольга Сергеевна
Российский экономический университет имени Г.В. Плеханова
студент

Аннотация
В статье рассматриваются особенности принципов действия биометрических систем и возникающие в них ошибки, которые делают биометрические системы уязвимыми. Для иллюстрации параметров биометрических систем и уязвимости представлены рисунки.
Ключевые слова: биометрия, биометрические системы, идентификация, верификация, биометрические уязвимости.

"Local" or "Stranger": influence of vulnerabilities on operability of biometric systems

Komarova Olga Sergeevna
Plekhanov Russian University of Economics
student

Abstract
The article discusses features of the principles of action of biometric systems and mistakes arising in them which do biometric systems vulnerable are considered. To illustrate parameters of biometric systems and vulnerability drawings are submitted.
Keywords: Biometrics, biometric systems, identification, verification, biometric vulnerabilities.

Несомненно, биометрия в настоящее время является наиболее востребованной областью для обеспечения безопасности. Биометрические системы считаются современной идей, однако данное утверждение неверно: ее основой пользовались египтяне, когда идентифицировали своих рабочих, которые строили великие пирамиды (различали работников не только по именам, но и по росту, телосложению, цвету лица и его форме и другим, наиболее явным отличиям). Но вопреки долгому времени, потребовавшегося для полноценной реализации данного метода, ряд объективных причин обуславливает интерес к биометрии. В обычных парольных системах (и в системах, где основу составляют карты доступа) угадывание пароля или его угадывание, изготовление дубликата приводит к компрометации системы. Пользователь же теряет возможность доступа к системе. Системы на основе биометрии почти лишены перечисленных недостатков, так как

идентификатор неразрывно связан с пользователем, потому изменение или потеря идентификатора происходят в чрезвычайных случаях, а сканеры современные биометрических данных обнаруживают использование подделок.

Основа биометрии заключается в решении вопросов **идентификации и верификации**.

Идентификация (сравнение «один ко многим») – поиск биометрической характеристики из ранее взятых, которая подходит к получаемой в этот момент времени биометрической характеристике. Обычно это последовательное сравнение полученной в данный момент характеристики со всеми хранящимися в базе данных. Требуемая для проверки степень подобия представляется в виде порога (установка корректного порогового значения ошибки двух родов, порог чувствительности является своеобразной гранью идентификации.), который регулируется для различного персонала, времени суток, мощности персонального компьютера и иных факторов. Следует учесть, в качестве результата либо выбирается наиболее похожая характеристика (идентификация прошла успешно), либо, если степень подобия оказалась наименьше заданной для всех сравнений, результат отсутствует.

Идентификация может выполняться как верификация, распознавание или аутентификация.

При верификации происходит подтверждение идентичности биометрического шаблона, хранимого в базе данных, и полученных данных.

При распознавании систему идентифицирует легитимного пользователя с соответствующим шаблоном, если один из шаблонов и полученные характеристики одинаковы.

При аутентификации идет подтверждение соответствия изображения, которое есть в видеокамере, с одним из находящихся в базе данных шаблонов.

Верификация (сравнение «один к одному») – проверка, что субъект (легитимный пользователь) есть именно тот, за кого себя выдает, то есть задача процесса состоит в том, чтобы убедиться, что полученная биометрическая характеристика соответствует ранее взятой.

Система «обучается» идентифицировать одного конкретного человека. Для создания цифрового представления человеческого облика, конкретные датчики (например, камера) сканируют человека, после чего формируется несколько изображений. Эти изображения могут иметь немного различные выражения лиц или ракурсы, что позволяет получить точные данные.

После чего из полученного образца программным алгоритмом экстракции черт (feature extractor) выявляют индивидуальные, характерные черты (пример: муниция – мелкие подробности линий пальца) [11, с 101]. Результат сохраняется системой в качестве шаблона в базе данных со всеми другими идентификаторами: идентификационный номер, имя, и т.д. В аутентификации легитимный пользователь предъявляет датчику дополнительный биометрический образец. Извлеченные из этого образца

черты впоследствии представляются запросом, который система алгоритмом сопоставления будет сравнивать с шаблоном заявленной личности. Алгоритм сопоставления возвращает рейтинг соответствия, показывающий степень равности между запросом и шаблоном. Система принимает заявление только в случае превышения заранее установленного порога рейтингом соответствия.

Работа биометрических систем происходит по одинаковой схеме.

1. Процесс записи, в результате которого система сохраняет образец биометрический характеристики. Некоторые системы для более подробного запоминания делают несколько образцов.

2. Обработка полученной информации и ее преобразование в математический код.

3. Использование биометрических методов идентификации и аутентификации пользователей.

Четыре стадии имеет идентификация по биометрической системе:

- регистрация идентификатора – скопление сведений поведенческой или физиологической характеристики, их преобразование в форму, которая будет доступна компьютерным технологиям, и сохранение в памяти биометрической системы;
- выделение – системой анализируется выделенные уникальные признаки из предъявляемого повторно идентификатора;
- сравнение – сопоставление сведений о предъявленном повторно уже зарегистрированном идентификаторе;
- решение – заключение о совпадение или отсутствии совпадений предъявленного заново идентификаторы.

Заключение о совпадениях или об отсутствии совпадений идентификатором может транслироваться иными системами, например, защитой информации или контролем доступа, которые будет действовать, исходя из полученной информации.

Одной из самых главных и важных характеристик системы защиты информации в биометрии – высокая надежность, чтобы нарушитель не смог выдать себя за легитимного пользователя (ошибочная позитивная идентификация), иначе система будет являться малопригодной.

Также необходимо исключить ошибки принятия системой законного пользователя за другого законного пользователя, биометрическая система должна доказать, что человек, предоставляющий свои биометрические характеристики, есть тот же самый человек, который регистрировался ранее, а не кто-то иной.

То есть, биометрической системе необходимо достоверно различать характеристики разных людей и надежно найти совпадения. Такими параметрами называются ошибка первого рода, ложного отказа (False Reject Rate, FRR) и ошибка второго рода, ложного допуска (False Accept Rate, FAR).

Сложная работа биометрических систем усложняется и тем, что возникают уязвимости, которые необходимо просчитать заранее и исключить

их или быть готовыми к их возникновению и иметь дополнительные меры для их устранения.

Два вида ошибок делают биометрическую систему уязвимой (рис. 1).

1. Возникает отказ в обслуживании, если системе не удается распознать легитимного пользователя.

2. Вторжение злоумышленником в биометрическую систему путем неверной идентификации в качестве авторизованного пользователя.

Множество возможных причин существует для данных сбоев, и они делятся **на атаки нарушителей и естественные ограничения**.

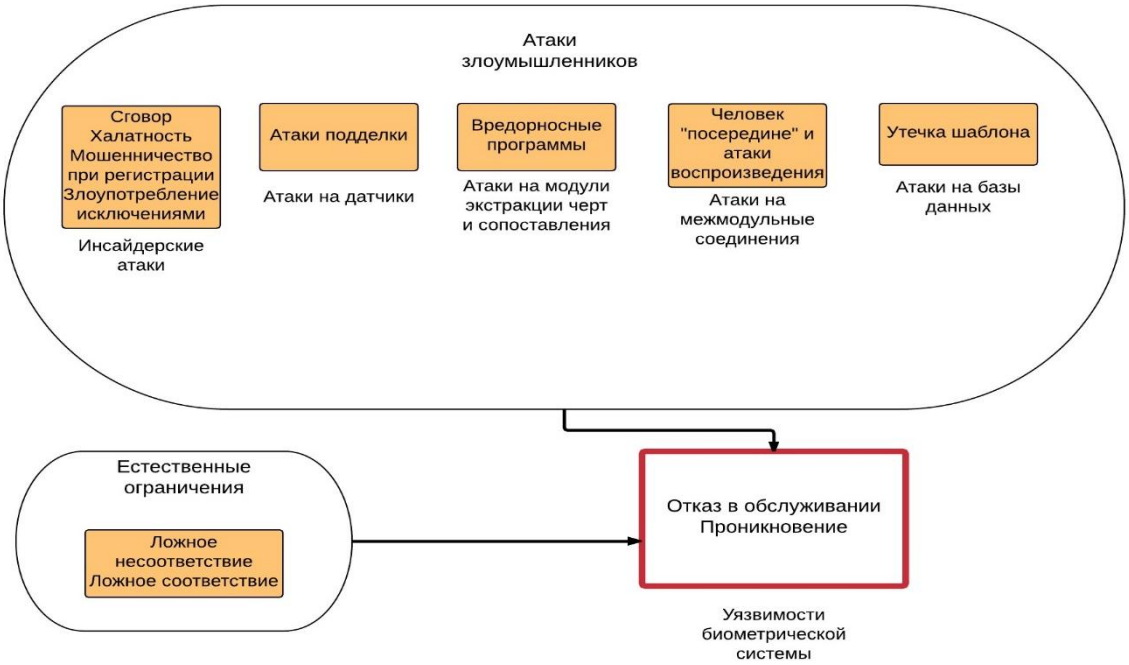

Рисунок 1 — Уязвимости биометрический системы

Естественные ограничения

Аутентификация биометрической системы отлична от обычных систем.

Если в системах аутентификации по паролю необходимо четкое соотношение не менее двух алфавитно-цифровых строк, то в биометрической аутентификационной системе проверяется степень идентичности двух биометрических образцов. Но так как приобретенные в ходе регистрации и аутентификации личные биометрические образцы не всегда схожи, (рис. 2) в биометрической системе возникают ошибки первого рода и второго рода.

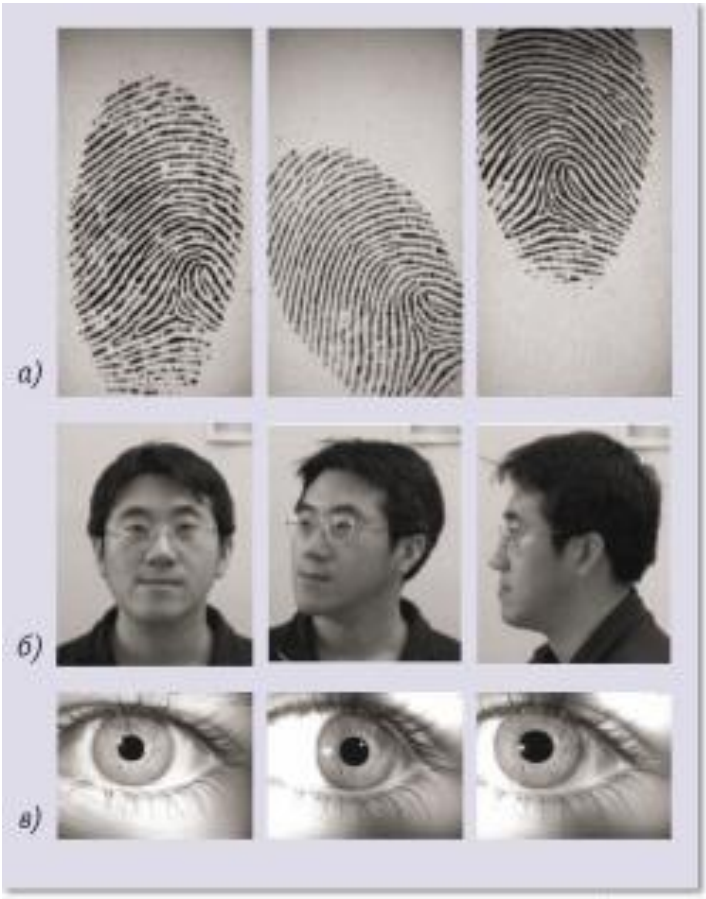

Рисунок 2 — Естественная вариабельность биометрических образцов человека

Исходя из рисунка 2 (а), видно, как варианты отпечатка одного и того же пальца при разном положении пальца отличны друг от друга; (б) — различные снимки ракурсов одного и того же лица; (в) — снимки радужной оболочки одного и того же глаза с сужением зрачка и изменением направления взгляда

Ошибка первого рода, ложный отказ (FRR) появляется, если сопоставленные образцы от одного человека системе не удается сравнить, потому что между собой у них наименьшая степень схожести.

Это вероятность принятия «своего» за «чужого», то есть в доступе «своему». Такая ошибка в коммерческих системах обычно выбирается равной около 0,01, потому что считается, если присутствует 1 процент подобных отказов, не критичной. Ее можно разрешить, позволив «своим» использовать несколько попыток (касаний) входа, и данным искусственным методом улучшить ошибку первого рода.

Но при большом потоке, чтобы не создавать очередей, во многих случаях приводятся специальные требования улучшений FRR до 0,001-0,0001.

Ошибка второго рода, ложный допуск (FAR) – если система, наоборот, неправильно признает образцы, полученные от разных людей, полностью идентичными, потому что они имеют между собой высокую схожесть.

Вероятность принять «чужого» за «своего» изменяется обычно в пределах от 10^{-3} до 10^{-6} (например, это означает, что 1 человек из 100 тыс. будет несанкционированно допущен, в % = 0,001), также есть решения с FAR = 10^{-9}. Чем больше данная ошибка, тем хуже, грубее система работает и возрастает возможность проникновения «чужого». Системы с большим количеством транзакций или пользователей, такие как, платежные системы, Интернет, должны ориентироваться на малые FAR-порядка: 10^{-9} и менее.

К отказу в обслуживании законного пользователя ведет ложный отказ. К атакам злоумышленника – ложный допуск, потому что для проникновения он не использует особые меры в обходе системы. Данный тип проникновения именуется «атакой нулевого усилия».

Ошибка ложного допуска (ложного пропуска) с точки зрения безопасности более опасна, но ошибка ложного отказа может привести к уменьшению удобства для пользования системой, которая может не распознать человека с первого раза.

Необходимо учитывать взаимосвязь данных вероятностей между собой, из-за искусственных попыток снизить уровень «требовательности» системы (FAR) уменьшается процент ошибок «чувствительности» (FRR) и наоборот, то есть, попытка уменьшения одной приводит к увеличению второй, поэтому на практике в зависимости от требований к системе выбирается определенный компромисс. Графики зависимости FRR и FAR от заданной точности сравнения предъявленного образца с шаблоном из базы данных показаны на рисунке 3.

Система с малым FAR хороши тем, что, ухудшая этот параметр, но, оставляя его еще достаточно хорошим, появляется возможность улучшить FRR.

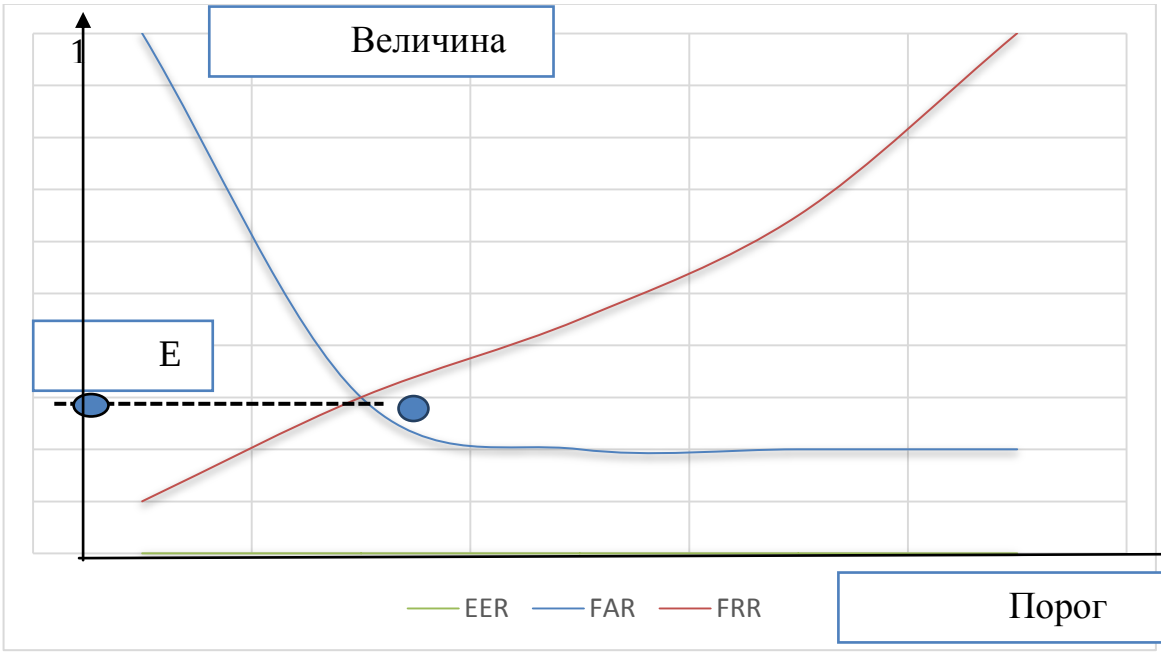

Рисунок 3 — Основные параметры биометрических систем

При высоких значениях благодаря заданной точности придерживается режим, когда ошибка первого рода (ложного отказа) значительно превосходит ошибку второго рода (ложного допуска), обеспечивая высокий уровень защиты.

Точка пересечения двух кривых коэффициент EER (равный уровень ошибок, Equal Error Rates или «CrossoverRate») – это уровень равной вероятности ошибок, такая величина характеризует качество использованного биометрического устройства (метода). В основном, устройства с низким EER наиболее точны. Чем меньше EER, тем более точной будет система [6, с 57].

Атаки злоумышленников

Также примерами возникновения ошибок и неполадок в биометрической системе служат манипуляции злоумышленников: через инсайдеров (например, системные администраторы), или методы прямой атаки на системную инфраструктуру. Обходов биометрических систем у внешних нарушителей есть несколько.

1. Сотрудничество с инсайдером (как добровольное, так и по принуждению со стороны злоумышленника).

2. Использование небрежного отношения к службе законным пользователем (человек не вышел из системы впоследствии окончания транзакции).

3. Манипуляции с процедурами обработки исключений и регистрации, созданные для оказания поддержки авторизованным пользователям.

4. Создавать сбои биометрических систем путем прямых атак на пользовательских интерфейс (датчик), модули экстракции черт или сопоставления либо баз шаблонов, либо на соединения между модулями.

К атакам на соединения между модулями, на их систему относятся: «человек посередине» (MITM-атака – атакующий читает и видоизменяет данные, обмениваемые корреспондентами друг с другом, никто из не подозревает присутствие взломщика), атаки воспроизведения или вредоносные компьютерные программы. Большое множество видов данных атак относятся и к системам аутентификации по паролю, поэтому применяются необходимые контрмеры наподобие криптографии, взаимной аутентификации или отметок времени, с их помощью предотвращается и уменьшается эффект атак нарушителей.

Наиболее важными, являющимися серьезными уязвимостями и способными нарушить защиту в биометрической системе, являются утечка из баз шаблонов и атака подделки на пользовательский интерфейс.

Атака подделки представляет собой подделывание биометрических образов живого человека. Например, отпечаток пальца, заимствованный с поверхности чего-либо или предмета, слепок лица.

Несмотря на легкий доступ к получению тех или иных биометрических признаков только потому, что осуществимо без особых трудностей получение скрытным образом фото лица человека, фундаментальный

признак в биометрической аутентификации неизменен – система остается защищенной, потому что признак физически связан с живым пользователем. Но успешными атаками подделки нарушается это базовое утверждение, тем самым сильно понижает уровень защищенности системы.

Ученные открыли множество подходов к определению живого состояния. Благодаря верификации физиологических характеристик непроизвольных, случайных факторов, таких, к примеру, как моргание, можно убедиться – зарегистрированная датчиком биометрическая особенность принадлежит человеку живому.

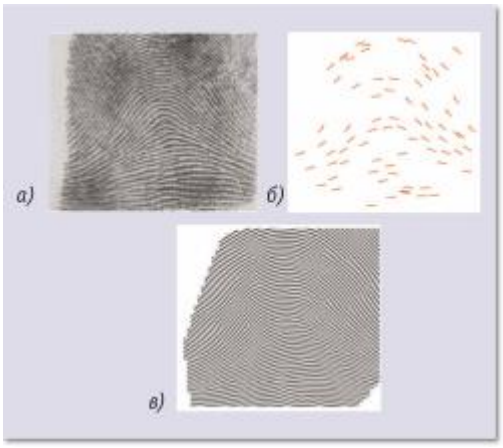

Рисунок 4 — Пример получения методом обратной инженерии соответствующего биометрического шаблона биометрической черты

Утечка из баз шаблонов происходит, когда данные о шаблоне законного пользователя становятся доступными нарушителю. Злоумышленнику удается восстановить биометрический рисунок, используя обратный инжиниринг шаблона (рис. 4), где из оригинального снимка отпечатка (рис. 4, а) изымается информация о линиях шаблона (рис. 4, б) и создается реконструированный образ отпечатка с использование только информации о линиях (рис. 4, в), и из-за этого увеличивается угроза подделывания.

Таким образом, можно сделать выводы:

1. Биометрическая система работает в пять этапов:

- получение биометрического образца (пример: отпечаток пальца) от пользователя;
- извлечение из него биометрические характеристики (например, особые точки и их параметры)
- сравнение данных характеристик с одним/несколькими характеристиками, хранящимися в базе данных;
- определение, насколько совпадают предъявленные характеристики с данными из базы

- заключение о том, удалось ли идентифицировать пользователя по полученным данным или проверить, что это именно тот, за кого он себя выдает.

2. При построении защиты биометрической системы необходимо учитывать вероятностные ошибки (FAR - точность, FRR - чувствительность), которые тесно связаны между собой.

3. При защите биометрической системе в первую очередь необходимо точно разрабатывать схемы защиты биометрических шаблонов, которые хранятся в базе данных. Возможность утечки шаблона повышает вероятность злоумышленнику проникнуть в базу и восстановить данные путём обратного инжиниринга.

Библиографический список

1. ГОСТ Р ИСО/МЭК19795-1-2007. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура.
2. Д. Брилюк, В. Старовойтов. Распознавание человека по изображению лица и нейросетевые методы. Публикация от 22-05-2015 на сайте по системам безопасности [Электронный ресурс] – http://www.Sec.ru. (дата обращения: 21.02.2018).
3. Вакуленко А., Юхнин А. Биометрические методы идентификации личности: обоснованный выбор и внедрение НПО ИНФОРМ, публикация на сайте «Российский биометрический портал» [Электронный ресурс] – http://www.biometrics.ru/ support/ biometrics/ about_biometrics.php. (дата обращения: 20.04.2018).
4. Глоссарий терминов интегрированных систем безопасности. Информационный сайт предприятия «Альфа-прибор» [Электронный ресурс] – www.alfa-pribor.ru. (дата обращения: 17.04.2018).
5. Лебеденко, Ю. И. Биометрические системы безопасности [Электронный ресурс] / Ю. И. Лебеденко. Тула: Издательство ТулГУ, 2015. 159с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=134536 (дата обращения 16.04.2018).
6. Довлетханов. Идентификации по радужке глаза. Публикация на сайте по системам безопасности [Электронный ресурс] http://www.Sec.ru. (дата обращения: 19.02.2018).
7. Ивантер Э.А., Коросов А.В. Элементарная биометрия: учебное пособие / Э.А. Ивантер: Петрозаводский ГУ. Петрозаводск: Изд-во ПетрГУ, 2015 104 с.
8. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации: учеб. Пособие для вузов; под ред. С.А. Клейменова. 3-е изд., стер.: Академия, 2016. 336 с.
9. Петрова О., Райлян А. Обзор существующих методов биометрической

идентификации / Публикация от 19.12.2014 г. на сайте по системамт безопасности [Электронный ресурс] http://www.Sec.ru. (дата обращения: 01.05.2018).
10. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. Пособие для вузов. М. : академия, 2012. 256с.
11. Anil K. Jain, Kathik Nandakumar, Biometric Authentication: System Security and User Privacy // IEEE Computer, November 2012, IEEE Computer Society. - 2016. С. 4—20.