УДК 57.087.1

# ОТМЕНЯЕМАЯ БИОМЕТРИЧЕСКАЯ СИСТЕМА БЕЗОПАСНОСТИ, ОСНОВАННАЯ НА ХАОТИЧЕСКИХ ФУНКЦИЯХ

**© 2022 Д. А. Ленская**

*студентка, направление подготовки Информационная безопасность*
*e-mail: svlrzm@yandex.ru*

*Российский технологический университет*

В настоящее время биометрические системы безопасности заменили систему аутентификации на основе пароля или токена во множестве областей. В связи с этим был принят ряд специализированных нормативных актов в сфере обеспечения безопасности биометрических данных: 152-ФЗ «О персональных данных», Постановление Правительства Российской Федерации № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», 149-ФЗ «Об информации, информационных технологиях и о защите информации». У биометрической системы аутентификации есть один очевидный минус: биометрические данные неизменны и остаются с человеком на протяжении всей его жизни, что, очевидно, накладывает на разработчиков системы безопасности колоссальную ответственность за соблюдение строжайшей конфиденциальности предоставляемых пользователем образцов. Так, существует феномен *отменяемой биометрии* [1], подразумевающий ее направленное и неоднократное искажение при регистрации и последующих идентификациях, что позволяет отозвать и аннулировать биометрический шаблон сродни паролю (биометрический шаблон – цифровое представление уникальных характеристик, которые были извлечены из биометрического образца и сохранены в биометрической базе данных). В ходе этого к каждой записи применяется свой метод искажения по специально разработанному алгоритму, что в случае утечки шаблона позволяет перерегистрировать новый вариант, изменив сам алгоритм. При этом процесс восстановления оригинала невозможен. За прошедшие годы был предложен ряд схем защиты биометрических шаблонов, основанных на принципе отменяемой биометрии [2]. В данной статье мы рассмотрим эффективность хаотических функций для генерации отменяемых биометрических шаблонов (хаотические функции используются вместо простого генератора случайных чисел, чтобы преодолеть потерю случайности в случае большого количества изображений).

**Ключевые слова:** биометрия, отменяемая биометрическая безопасность, аутентификация, хаотические функции, распознавание отпечатков пальцев.

# REPEALABLE BIOMETRIC SECURITY SYSTEM BASED ON CHAOTIC FUNCTIONS

**© 2022 D. A. Lenskaya**

*Student of the the Direction of training Information security*
*e-mail: svlrzm@yandex.ru*

*Russian Technological University*

Repealable Biometric security System Based on Chaotic Functions Annotation Currently, biometric security systems have replaced the password- or token-based authentication system in a variety of areas. In this regard, a number of specialized regulations were adopted in the field of biometric data security: 152-FZ "On Personal Data", Decree of the Government of the Russian Federation No. 512 "On Approval of Requirements for Material Carriers of Biometric Personal Data and technologies for Storing such data outside of Personal Data Information Systems", 149-FZ "On Information, information technologies and information protection". So, the biometric authentication system has one obvious disadvantage: biometric data is unchanged and remains with a

person throughout his life, which obviously imposes on the developers of the security system a huge responsibility for observing the strictest confidentiality of the data provided.

**Keywords:** biometrics, revocable biometric security, authentication, chaotic functions, fingerprint recognition.

**Введение**

В связи с быстрым развитием передовых информационных технологий, облачных вычислений и приложений Интернета Вещей защита и безопасность индивидуальных данных приобрели необычайную важность. Основными трудностями в рамках системы проверки являются проверка кодов, индивидуальных распознаваемых идентификационных номеров подтверждения, то есть PIN-кодов, и паролей. Таким образом, биометрические характеристики используются в различных приложениях как логичный шаг по усовершенствованию подтверждения, проверки и распознавания личности.

Основная функция этих биометрических систем включает в себя выбор биометрических данных. После этого объекты извлекаются и сохраняются в наборах данных. Биометрические схемы для защиты физиологических характеристик людей, таких как черты лица, радужной оболочки глаза и отпечатков пальцев, становятся широко распространенными. Проблема в том, что клиенты используют биометрические данные постоянно и не могут их изменить. Кроме того, украденные биометрические данные могут быть использованы в сценарии перекрестной координации. Поэтому рекомендуется применять необратимые преобразования для предотвращения кражи биометрических данных.

**1. Биометрическое соление и необратимое преобразование**

Для безопасного хранения паролей используются два ключевых элемента: хэширование и соление [3]. Просто хэширование не является безошибочным вариантом, потому что может быть успешно побеждено атаками по словарю или по радужной таблице, ведь люди склонны выбирать для паролей одни и те же слова и осмысленные выражения. Одним из способов защиты от этого является добавление соли или использование соленых паролей. Соление – это процесс добавления серии случайных символов к паролю перед выполнением функции хеширования.

*Биометрическая соль* следует тому же принципу, что и пользовательский и независимый входной фактор (вспомогательные данные, такие как пароль или случайные числа пользователя), она смешивается с биометрическими данными для получения искаженной версии биометрического шаблона. Поскольку вспомогательные данные получены извне и напрямую взаимодействуют с биометрическими данными, они могут быть легко изменены и отозваны и потому должны храниться в тайне для максимальной защиты безопасности. Однако, поскольку внешние конфиденциальные ключи или пароли легко могут быть потеряны, украдены или скомпрометированы, точность и уязвимости существующих схем должны быть оправданы.

В *необратимом преобразовании* функция $f$ предназначена для преднамеренного изменения необработанного биометрического изображения в новую форму в контексте пространства признаков или сигналов. Функция $f$ служит агентом в контексте безопасности шаблонов, обеспечивая необратимость, повторное использование и разнообразие шаблонов. Поскольку $f$ не имеет прямого взаимодействия с необработанной биометрией, основным преимуществом такого подхода является то, что $f$ не нужно держать в секрете [4].

## 2. Хаотические функции

*Хаотическая функция* – это функция, чье доменное (входное) пространство и диапазон (выходное) пространство хаотичны. Реализация *криптографии*, основанной на хаосе, зависит от хаотических функций. Хаотические функции представляют собой класс динамических систем, в которых время дискретно, а не непрерывно. Они демонстрируют хаотичное поведение при определенных значениях параметров. В данном исследовании будут использованы две функции: логистическая и квадратическая.

*Логистическая функция* – это нелинейная динамическая функция, уравнение которой выглядит следующим образом:

$$x_{n+1} = \mathrm{r}x_n(1 - x_n) \quad (1)$$

где $x_n$ – значение от 0 до 1, n – индекс итерации, а r – положительное число от 0 до 4.

*Квадратическая функция* – значимый пример хаотической системы. Она задается следующим образом:

$$x_{n+1} = r - a{x_n}^2 \quad (2)$$

где r – параметр хаотической функции, а – константа, а n – индекс итерации [5].

## 3. Шифрование на основе ядер свертки

Предлагаемая схема шифрования реализуется посредством свертки со случайным ядром, генерируемым с использованием ключа, связанного с простым изображением. Ядро свертки генерируется с помощью одной из хаотических функций. Процесс шифрования выполняется посредством операции свертки между случайным ядром и изображением отпечатка пальца [6].

## 4. Биометрическая система с возможностью отмены на основе хаоса

Чтобы защитить биометрические данные пользователей от хакеров и гарантировать возможность создания отменяемых шаблонов, биометрические данные должны быть зашифрованы. Таким образом, в случае кражи или потери мы можем получить другой зашифрованный биометрический шаблон из того же исходного биометрического шаблона. Шифрование изображений на основе хаоса очень подходит для шифрования биометрических шаблонов, поскольку хаотические функции очень чувствительны к начальным условиям. При внесении небольших изменений в начальные условия хаотической функции радикально изменяется полученная зашифрованная биометрия, которую можно повторно использовать в одном и том же приложении. Если отменяемые биометрические данные украдены, они могут быть выданы повторно.

### 4.1. Архитектура отменяемой биометрической системы

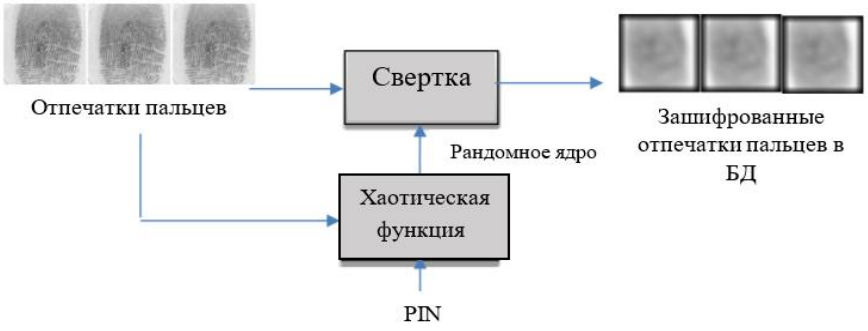


Рис. 1. Этап регистрации для отменяемых биометрических шаблонов

Биометрическая система с возможностью отмены делится на два этапа: фаза регистрации и фаза аутентификации. На этапе регистрации (рис. 1) устройство захвата отпечатков пальцев используется для генерации изображений отпечатков пальцев. Затем эти изображения свертываются с помощью ядра случайной свертки. В данной схеме ядро сгенерировано с помощью PIN-кода пользователя, то есть для генерации ядра случайной свертки в качестве начального условия используется PIN-код. Это ядро случайной свертки свертывается с обучающими изображениями для создания зашифрованных обучающих шаблонов. Полученные зашифрованные обучающие шаблоны можно поместить на карту и впоследствии использовать для проверки идентификаторов пользователей. Если карта потеряна или украдена, можно создать альтернативное ядро упаковки для создания различных закодированных биометрических шаблонов. Если злоумышленник попытается использовать украденную карту, чтобы восстановить биометрические данные пользователя, ему или ей необходимо знать ядро обхода, используемое на этапе записи. Для того чтобы хакеры могли получить исходную модель, необходимо выполнить декодирование изображения, что невероятно сложно выполнить, не зная PIN-код клиента и шифровальную схему. Следовательно, это рассматривается как значительная степень безопасности для биометрических шаблонов.

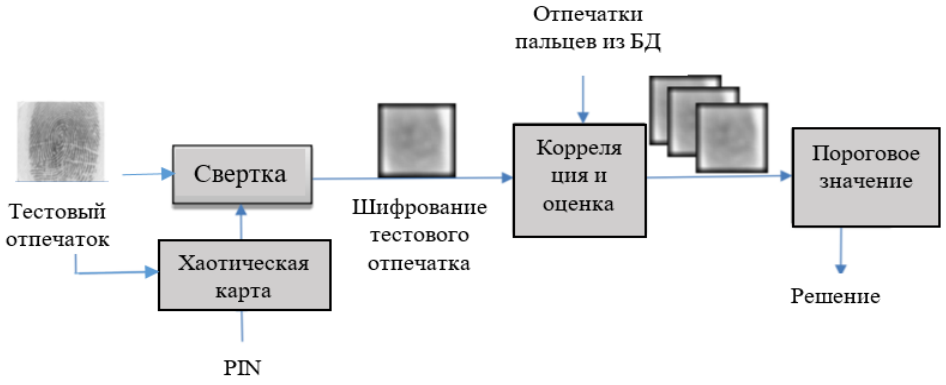


Рис. 2. Этап аутентификации для отменяемых биометрических шаблонов

На этапе аутентификации (рис. 2) пользователь представляет зашифрованный отпечаток пальца таким же образом, как и на этапе регистрации. Тестовые изображения сопоставляются с сохраненными шаблонами. Распределения генерируются для оценок корреляции в подлинных и поддельных тестах. Следовательно, определяется пороговое значение для процесса утверждения для пользователей [7].

**4.2. Показатели аутентификации**

Чтобы обеспечить сходство между тестовым зашифрованным отпечатком пальца и зашифрованным биометрическим шаблоном в наборе данных, используется оценка корреляции. Чем выше значение корреляции, тем выше сходство между паттернами. Если индивидуальный показатель корреляции превышает определенный порог, допуск к системе подтверждается. Оценки неутвержденных пользователей должны быть неизменно ниже, чем у одобренных пользователей [8].

Из-за различных причин в биометрических системах могут происходить некоторые ошибки в расположении. Например, неутвержденные шаблоны могут создавать оценки выше, чем у некоторых утвержденных шаблонов.

Пороговое значение может быть выбрано таким образом, чтобы гарантировать, что все неутвержденные баллы не превышают заданного порогового значения. Следовательно, система ошибочно не распознает никаких шаблонов. Кроме того,

утвержденные шаблоны с оценками ниже заданного порогового значения ошибочно отклоняются.

Следовательно, мы можем выбрать пороговое значение, чтобы ни один авторизованный шаблон не был отклонен ошибочно. В этом случае некоторые неутвержденные объекты распознаются ошибочно. Как правило, в системе биометрической проверки тестовая информация содержит одобренные и неутвержденные шаблоны. Баллы по каждому из утвержденных и неутвержденные примеры будут так или иначе распространяться вокруг средства распространения. Средний балл утвержденных шаблонов выше, чем у неутвержденных шаблонов.

Следовательно, инструменты, которые можно использовать для проверки полученных оценок, – это вероятность истинного распределения (PTD) и вероятность ложного распределения (PFD) оценок корреляции, полученных на этапе валидации. PTD – это вероятность корреляции между авторизованными отпечатками пальцев и закодированными биометрическими шаблонами в базах данных, в то время как PFD (неутвержденные образцы) – это вероятность корреляции между несанкционированным отпечатком пальца и теми, которые хранятся в базе данных. Мы разрешаем доступ к системе, если новый результат отпечатка превышает заданный порог с определенной вероятностью ошибки. Вероятность правильного обнаружения может быть легко получена из вероятности ошибки, и мы можем получить лучшую производительность системы при более низких вероятностях ошибок.

**5. Результаты эксперимента**

В исследовании [6], на которое мы опирались, были проведены эксперименты по моделированию на 20 различных отпечатках пальцев для 20 человек. Каждый отпечаток пальца имеет размер 300 × 300 пикселей. Используются квадратические и логистические хаотические функции с ключами, связанными с простыми изображениями. Было показано, что наибольшую точность с практически неограниченным разнообразием возможных PIN-кодов дает квадратическая функция, заданная следующий образом:

$$x_{n+1} = \mathrm{r} + (1 - 8x_n)^2 \quad (3)$$

Ключи используются для генерации ядер случайной свертки. Начальные условия этих хаотических функций изменяются в соответствии с PIN-кодом, который представляет каждый пользователь. Наконец, мы сравниваем все хаотические функции. На этапе регистрации пользователь вводит свой собственный PIN, и это создает эквивалентные ядра, которые свернуты с обучающими изображениями. Полученные в результате 20 зашифрованных биометрических шаблонов сохраняются в базе данных.

На этапе аутентификации мы используем два отпечатка пальцев для тестирования. Один из них принадлежит авторизованным пользователям, а другой – неавторизованным. В обоих случаях тестируемый пользователь вводит PIN-код и создает ядро случайного переноса. Следовательно, мы получаем два закодированных отпечатка пальцев для теста. Мы предполагаем, что неавторизованное лицо знает правильный PIN-код для авторизованного пользователя для проверки безопасности системы. Мы получаем значения корреляции между двумя зашифрованными отпечатками пальцев и 20 сохраненными зашифрованными биометрическими шаблонами. Вероятности истинного и ложного распределения отображаются для отменяемых биометрических систем для всех хаотических функций, чтобы определить порог ошибки и вероятность. Пересечение двух кривых определяет пороговое значение, в соответствии с которым мы можем определить, авторизован пользователь или нет. На этапе регистрации пользователь вводит свой собственный

PIN, и это создает соответствующее ядро, которое свертывается с помощью отпечатка пальца.

**6. Вывод**

Итак, мы рассмотрели эффективность хаотических функций для генерации отменяемых биометрических шаблонов. Было показано, что использование предложенной квадратической функции 3 в отменяемой биометрической системе приводит к наименьшей вероятности ошибки среди всех систем с различными хаотическими функциями. Схемы шифрования и хеширования регулярно используются для защиты биометрических шаблонов. С этими стратегиями связаны две проблемы. Во-первых, закодированные биометрические данные должны быть декодированы для распознавания. Если биометрические данные расшифрованы, это дает шанс для попыток взлома. Другая проблема заключается в том, что незначительные изменения в биометрических данных серьезно влияют на хэш-функции. Следовательно, эти функции на практике не могут быть использованы напрямую. Концепция отменяемой биометрии вводится в этой статье в качестве решения этих двух проблем. Здесь был представлен метод для создания зашифрованных биометрических шаблонов, которые могут быть изменены с использованием различных ядер свертки, генерируемых различными хаотическими функциями. Использование зашифрованных данных в биометрических системах позволяет осуществлять процесс проверки непосредственно с помощью корреляционного теста. Даже если злоумышленнику удастся украсть зашифрованные биометрические шаблоны, ему потребуется произвести обратную свертку со случайным ядром, сгенерированным с помощью определенного ключа.

***Библиографический список***

1. *Горшков, А. А.* Как защитить биометрические данные пользователей от криминального использования / А. А. Горшков (19.05.2020). — URL: https://rb.ru/opinion/biometric-data-protection (дата обращения; 13.04.2022).
2. *Ксинбо Донг, Жэ Джин, Э. Бэнг Джин Тео, Массимо Тистарелли, Кокшейк Вонг.* О риске безопасности, связанном с отменяемыми биометрическими данными, 2020. — URL: https://arxiv.org/pdf/1910.07770.pdf (дата обращения; 13.04.2022).
3. *Э.Т.Бэнг Джин, Лим Мэнг Уи.* Отменяемая биометрика, 2010. — URL: http://www.scholarpedia.org/article/Cancelable_biometrics
4. *Джейсон Джунг.* Соление и хэширование паролей, 2021. — URL: https://www.okta.com/blog/2019/03/what-are-salted-passwords-and-password-hashing/ (дата обращения; 13.04.2022).
5. *Вафаа Сабер АбделХалим Саид*. Генерализованные хаотические функции между анализом и внедрением, 2015. — URL: http://eece.cu.edu.eg/~hfahmy/thesis/2015_09_chaos.pdf (дата обращения; 13.04.2022).
6. *А. Абдэл-Хамид, Ноа Рамадан, Валид Эл-Шафаи Менуфиа, Ашраф А.М. Халаф.* Отменяемые биометрические системы безопасности // The Visual Computer, 2021
7. *Аарти Лаксман Гилбил, Прамонд Д. Ганжевар.* Проектирование защищенной биометрической системы с использованием отменяемых методов // Конспекты лекций в серии книг по электротехнике (LNEE. Том 783). – 2021. – С. 717–726.

8. Основные параметры биометрических систем. — URL: https://www.telecamera.ru/content/articles/s6657/e47708/ (дата обращения; 13.04.2022).
9. ISO/IEC 24745-2022 Информационная безопасность, кибербезопасность и защита приватности — Защита биометрических данных