Федоренко Б.Н. Этические и конфиденциальные аспекты биометрии в информационной безопасности// Международный журнал информационных технологий и энергоэффективности. – 2024. –
Т. 9 № 2(40) С. 91–96

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056.5

ЭТИЧЕСКИЕ И КОНФИДЕНЦИАЛЬНЫЕ АСПЕКТЫ БИОМЕТРИИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Федоренко Б.Н.
ФГАОУ ВО "РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА", Москва, Россия (127055, город Москва, ул. Образцова, д.9 стр.9), e-mail: xbogdan1349x@gmail.com

Статья обсуждает этические и конфиденциальные аспекты использования биометрии в информационной безопасности. Она рассматривает различные виды биометрических данных, включая отпечатки пальцев, голос, лицо, сетчатку глаза и стиль набора текста. В статье подчеркивается важность баланса между обеспечением безопасности и защитой прав и свобод индивидуума. Она также обсуждает важность прозрачности в использовании и хранении биометрических данных, а также необходимость соблюдения законов и регуляций о конфиденциальности. В заключении подчеркивается важность этичного и ответственного использования биометрии в информационной безопасности.

Ключевые слова: Биометрия, информационная безопасность, этика, конфиденциальность, отпечатки пальцев, голосовая биометрия, биометрия лица, сетчатка глаза, стиль набора текста, шифрование.

ETHICAL AND CONFIDENTIAL ASPECTS OF BIOMETRICS IN INFORMATION SECURITY

Fedorenko B.N.
RUSSIAN UNIVERSITY OF TRANSPORT, Moscow, Russia (127055, Moscow, Obraztsova st., 9, bldg. 9), e-mail: xbogdan1349x@gmail.com

The article discusses the ethical and confidential aspects of the use of biometrics in information security. She examines various types of biometric data, including fingerprints, voice, face, retina, and typing style. The article emphasizes the importance of a balance between ensuring security and protecting individual rights and freedoms. She also discusses the importance of transparency in the use and storage of biometric data, as well as the need to comply with privacy laws and regulations. In conclusion, the importance of ethical and responsible use of biometrics in information security is emphasized.

Keywords: Biometrics, information security, ethics, privacy, fingerprints, voice biometrics, facial biometrics, retina, typing style, encryption.

Введение

Биометрические технологии, ключевой инструмент в современной информационной безопасности, стали неотъемлемой частью нашего быта. Они проникли во многие аспекты нашей жизни, начиная от разблокировки персональных устройств, таких как смартфоны, и заканчивая обеспечением доступа к рабочим пространствам [1]. Биометрия играет важную роль в процессах идентификации и аутентификации пользователей, предоставляя решения, которые в корне отличаются от традиционных подходов.

Эти технологии предоставляют ряд уникальных преимуществ по сравнению с классическими методами аутентификации, такими как пароли или PIN-коды [2]. Главным из них является удобство для конечного пользователя: нет необходимости запоминать сложные и часто забываемые пароли. Биометрические данные, будь то отпечатки пальцев, сканирование радужной оболочки глаза или распознавание лица, предлагают более высокий уровень безопасности. Они труднее подделать и украсть, что делает их надежным инструментом защиты персональных и корпоративных данных.

Однако, несмотря на эти преимущества, существуют и вопросы, связанные с этикой и конфиденциальностью данных. По мере расширения применения биометрических технологий, возрастает и актуальность этих вопросов. Важно не только понимать возникающие проблемы, но и активно обсуждать их, чтобы обеспечить ответственное и этичное использование биометрии в сфере информационной безопасности. В данной статье ставится задача провести такое обсуждение, выявить ключевые моменты и предложить пути их решения.

Биометрия и информационная безопасность

В современной сфере информационной безопасности биометрия занимает ведущие позиции. Эта технология опирается на уникальные физиологические или поведенческие особенности человека для проведения идентификации и аутентификации. К примеру, в эту категорию входят такие данные, как отпечатки пальцев, голос, черты лица, рисунок сетчатки глаза и даже индивидуальный стиль печатания [3].

Отпечатки пальцев, которые, пожалуй, являются самым распространенным видом биометрических данных, обладают уникальностью для каждого человека и не меняются с течением времени, что делает их идеальным инструментом для систем безопасности. Их применение варьируется от разблокировки смартфонов до систем контроля доступа, при этом они удобны в использовании и обеспечивают высокий уровень безопасности за счет трудности подделки и кражи.

Голосовая биометрия основывается на уникальных характеристиках голоса, включая тембр, интонацию, скорость речи и другие параметры. Этот вид биометрии особенно удобен, когда другие методы недоступны или неудобны, например, в ситуациях, где использование рук для ввода данных ограничено.

Биометрия лица, использующая различные черты лица, такие как расстояние между глазами, форма носа и контур губ, стала широко распространена благодаря развитию технологий машинного обучения и искусственного интеллекта. Этот метод находит применение в различных областях, от мобильных устройств до систем контроля доступа в зданиях и на рабочих местах.

Сканирование сетчатки глаза, предлагающее высокую степень точности благодаря уникальному узору кровеносных сосудов, используется в особо защищенных установках, таких как военные базы или исследовательские лаборатории. Однако, его применение порождает вопросы конфиденциальности и этических соображений.

Клавиатурная динамика, или анализ стиля набора текста, представляет собой относительно новый вид биометрии. Он включает анализ таких параметров, как скорость печатания, сила нажатия на клавиши и интервал между нажатиями, создавая уникальный

"профиль печатания" пользователя. Этот метод особенно полезен для обнаружения несанкционированных входов или мошенничества в онлайн-системах.

Все эти методы биометрии обеспечивают высокий уровень безопасности, но в то же время порождают ряд вопросов, связанных с этикой, конфиденциальностью и защитой данных. Эти вопросы затрагивают проблемы свободы выбора, прозрачности использования данных, их конфиденциальности и безопасности, и они требуют тщательного обсуждения и внимания со стороны всех участников процесса - от конечных пользователей и разработчиков до законодателей и регулирующих органов.

Этические вопросы

Применение биометрии в области информационной безопасности порождает ряд непростых этических дилемм, которые требуют вдумчивого анализа и решения.

Первая проблема касается свободы выбора индивидов. Биометрическая идентификация тесно связана с личными данными человека. В этом контексте люди могут оказаться перед выбором: предоставить свои биометрические данные для получения доступа к некоторым услугам или местам или отказаться от этого. Некоторые могут испытывать дискомфорт или ощущать угрозу своей конфиденциальности при предоставлении таких чувствительных сведений. Очень важно предоставить возможность выбора между использованием биометрии и альтернативными методами аутентификации [4].

Вторая проблема связана с прозрачностью обработки данных. Пользователям важно быть в курсе того, как используются их биометрические данные. Это включает информацию о способах сбора, использования, обращения и защиты данных, а также о возможных рисках, связанных с их обработкой.

Третья проблема заключается в потенциальной дискриминации и справедливости. Биометрические системы могут работать с разной степенью точности для различных групп населения. Например, системы распознавания лиц могут быть менее эффективны для людей с определенными типами кожи или для тех, кто перенес значительные изменения во внешности. Это может привести к неравному доступу к услугам и возможностям.

Четвертая проблема касается приватности и неприкосновенности частной жизни. Биометрические данные являются чрезвычайно личными и могут влиять на чувство конфиденциальности и неприкосновенности личной жизни. Например, использование биометрии для мониторинга или слежения может быть воспринято как вторжение в личную сферу.

Решение этих вопросов требует участия и внимания всех заинтересованных сторон - от конечных пользователей и разработчиков до законодателей и контролирующих органов. Это необходимо для гарантии этичного и ответственного применения биометрии в сфере информационной безопасности.

Конфиденциальность

Конфиденциальность является одним из самых критически важных аспектов при работе с биометрическими данными. Биометрические данные представляют собой уникальную и крайне чувствительную информацию, которая относится к конкретному человеку и не может быть изменена или воспроизведена, как это возможно с паролями или номерами карт.

Организации, занимающиеся сбором и использованием биометрических данных, обязаны придерживаться строгих мер безопасности для защиты этих данных. Это включает в себя использование мощных методов шифрования, чтобы предотвратить несанкционированный доступ к данным. Кроме того, организации должны обеспечивать безопасное хранение биометрических данных и предоставлять доступ к ним только авторизованным пользователям.

Также важно, чтобы организации были прозрачными в отношении использования и хранения биометрических данных. Пользователи имеют право знать, как именно их данные используются, и должны иметь возможность контролировать этот процесс. Это может включать в себя право на отказ от использования биометрии или даже на удаление своих биометрических данных из системы.

Кроме того, организации должны учитывать законодательные аспекты конфиденциальности. В разных странах существуют разные законы и регуляции, касающиеся сбора, хранения и использования биометрических данных. Поэтому важно, чтобы организации обеспечивали соблюдение всех соответствующих законов и регуляций, действующих в их юрисдикции.

Наконец, следует учитывать вопросы, связанные с приватностью и неприкосновенностью частной жизни. Использование биометрии для слежения или мониторинга может вызвать опасения относительно вмешательства в личную жизнь [5]. Поэтому важно проводить открытый диалог и обсуждение между всеми заинтересованными сторонами, включая пользователей, разработчиков, законодателей и регуляторов. Это поможет установить баланс между использованием биометрии в информационной безопасности и уважением к приватности и правам личности, обеспечивая этичное и ответственное применение этой технологии.

Выводы

Биометрия играет важную роль в информационной безопасности. Она предлагает уникальные преимущества по сравнению с традиционными методами аутентификации, такими как пароли или PIN-коды. Однако, вместе с этими преимуществами возникают вопросы этики и конфиденциальности.

Важно учесть эти этические и конфиденциальные аспекты при использовании биометрии. Это требует баланса между обеспечением безопасности и защитой прав и свобод индивидуума. Это включает в себя уважение к свободе выбора, прозрачности, конфиденциальности и неприкосновенности частной жизни.

Организации, которые используют биометрические данные, должны принимать строгие меры для защиты этих данных. Это включает в себя использование сильных методов шифрования, безопасное хранение данных и ограничение доступа к данным только для авторизованных пользователей.

Кроме того, организации должны быть прозрачными в отношении того, как они используют и хранят биометрические данные. Пользователи имеют право знать, как их данные используются, и должны иметь возможность контролировать использование своих данных.

В заключение, биометрия является мощным инструментом в области информационной безопасности. Однако, как и любая технология, она должна использоваться ответственно. Это

включает в себя учет этических и конфиденциальных аспектов, а также обеспечение защиты и уважения прав каждого индивидуума. Это обсуждение является важным шагом в этом направлении.

Список литературы

1. Стольников Е.А., Влох Д.Д. Использование биометрии в информационной безопасности // Современные научные исследования и инновации. — 2023. — № 9. — [Электронный ресурс]. URL: https://web.snauka.ru/issues/2023/09/100808 (дата обращения: 10.01.2024).
2. Корнев, Л. В. Методы биометрии при обеспечении информационной безопасности / Л. В. Корнев. — Текст : электронный//Молодой ученый. — 2022. — № 17 (412). — С. 358-361. — URL: https://moluch.ru/archive/412/90789/ (дата обращения: 10.01.2024).
3. Чернобровов, А. Биометрические системы и персональные данные: как это работает и чем угрожает/А.Чернобровов — Текст: электронный.—URL: https://chernobrovov.ru/articles/biometricheskie-sistemy-i-personalnye-dannye-kak-eto-rabotaet-i-chem-ugrozhaet.html (дата обращения: 10.01.2024).
4. Мамаев, В. Этичная биометрия/В.Мамаев — Текст: электронный — URL: https://www.secuteck.ru/articles/ehtichnaya-biometriya (дата обращения: 10.01.2024).
5. Андерсон Н. Что такое биометрия и как она обеспечивает безопасность?/Н.Андерсон — Текст: электронный. — URL: https://fastestvpn.com/ru/blog/%D1%87%D1%82%D0%BE-%D1%82%D0%B0%D0%BA%D0%BE%D0%B5-%D0%B1%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F-%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C (дата обращения: 10.01.2024).

References

1. Stolnikov E.A., Vlokh D.D. The use of biometrics in information security // Modern scientific research and innovations. — 2023. — No. 9. — [Electronic resource]. URL: https://web.snauka.ru/issues/2023/09/100808 (date of reference: 10.01.2024).
2. Kornev, L. V. Methods of biometrics in ensuring information security / L. V. Kornev. — Text: electronic // Young scientist. — 2022. — № 17 (412). — Pp. 358-361. — URL: https://moluch.ru/archive/412/90789 / (date of access: 10.01.2024).
3. Chernobrovov, A. Biometric systems and personal data: how it works and what it threatens / A. Chernobrovov — Text : electronic. — URL: https://chernobrovov.ru/articles/biometricheskie-sistemy-i-personalnye-dannye-kak-eto-rabotaet-i-chem-ugrozhaet.html (date of reference: 10.01.2024).
4. Mamaev, V. Ethical biometrics / V. Mamaev — Text : electronic. — URL: https://www.secuteck.ru/articles/ehtichnaya-biometriya (date of application: 10.01.2024).
5. Anderson, N. What is biometrics and how does it ensure security? / N. Anderson — Text : electronic. — URL: https://fastestvpn.com/ru/blog/%D1%87%D1%82%D0%BE-%D1%82%D0%B0%D0%BA%D0%BE%D0%B5-%D0%B1%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F-

%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C (date of application: 10.01.2024).