

ОПАСНОСТЬ УТЕЧКИ БИОМЕТРИЧЕСКИХ ДАННЫХ

Бойков Илья Александрович

студент, Московский государственный технический университет им. Н. Э. Баумана, РФ, г. Москва

Цыганок Дарья Игоревна

студент, Московский государственный технический университет им. Н. Э. Баумана, РФ, г. Москва

Одной из главных проблем в сфере информационной безопасности с переходом в информационный век стала киберпреступность. Вследствие чего были придуманы методы защиты с использованием биометрических данных. Но для этого нужна была законодательная база, которая должна объяснить, что можно считать биометрическими данными и как их нужно охранять.

В России для обработки и хранения этих данных был принят закон «Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) "О персональных данных"» [1]. В котором сказано: «Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность [1].

Из этой же статьи следует что, такие данные собираются и обрабатываются только с согласия человека. «Используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных»

В настоящее время в России для сбора биометрии и ее использования для идентификации пользователей финансовых услуг работает Единая биометрическая система (ЕБС). Она не пользуется большой популярностью: в феврале 2021 года в ней было зарегистрировано около 164 тысяч россиян (чуть более 0,1% населения страны). Банки и страховые компании являются основными партнерами ЕБС.

Половина россиян, опрошенных НАФИ в декабре 2020 года, не доверяют ЕБС и вообще сбору биометрических данных. [2] Вместе с тем уже сейчас в тестовом режиме есть оплата «по лицу» в некоторых продуктовых магазинах и транспортных хабах.

На данный момент биометрические данные можно разделить на три группы. Фальсификация возможна: отпечаток пальца, распознавание лица 2D, распознавание лица 3D, распознавание голоса. Безуспешна: радужная оболочка глаза. Невозможна: сетчатка глаз, рисунок вен.

Заместитель министра финансов РФ Алексей Моисеев в своем интервью сказал: «Компрометация биометрических данных — это самое страшное, что может произойти. Если человек доверил экосистеме — неважно, частной или государственной — свои биометрические данные, и эта система не оправдала его доверия, то у человека в цифровом будущем сломана жизнь. Можно поменять пин-код на карточке, можно поменять паспорт, все что угодно, можно поменять фамилию и так далее. Но поменять биометрические данные... наверное, можно, но большинство людей, наверное, посчитает слишком большой издержкой изменить лицо или еще что-то» [3]

Первые существенные хищения выявленные за период 2016-2019 год:

2016	1. В Гане похищены биометрические данные избирателей. [4]
2017	1. Украдены биометрические данные филиппинских избирателей. [5] 2. У американской компании Avanti Markets, похищены отпечатки пальцев покупателей [6] 3. Утечка данных из индийской биометрической системы Aadhaar. [6]
2018	1. В Зимбабве похитили отпечатки пальцев и фотографии избирателей. [7] 2. Компрометация биометрических данных миллиарда граждан Индии. [8]
2019	1. В открытый доступ попала многомиллионная база отпечатков пальцев из южнокорейской Suprema. [9] 2. Похищены записи голоса клиентов Сбербанка. [10]

Для исключения и минимизации возможного ущерба, необходимо оперативно выявлять попытки имитации чужой биометрии — обнаруживать подделку в реальном времени и подтверждать или опровергать, что данные представлены их обладателем. Проверка на живой/неживой с использованием многофакторной идентификации значительно повышает безопасность и снижает ущерб от кражи персональных данных.

Реализовав многофакторное решение, когда регистрируются несколько биометрических и не биометрических признаков личности, можно обеспечить качественную и надежную идентификацию пользователей. Данная концепция заключается в объединении биометрических данных с другими элементами безопасности. Данные решения создают более надежные цифровые учетные записи, тем самым украденных биометрических признаков становится недостаточно для совершения противоправных действий.

Необходимо использовать сочетание нескольких надежных способов идентификации, чтобы пользователь сам мог выбрать наиболее приемлемые и удобные для него.

Биометрические данные неизменны поэтому нельзя допустить их утечку, так как потеряв их в момент, когда данная технология только начинает набирать обороты, можно навсегда лишиться возможности пользоваться ими в дальнейшем. В связи с этим, стоит не торопиться со сдачей биометрических данных. Государство и компании должны гарантировать полную защиту биометрических данных, так как их потеря или кража может нанести больше урона, чем защита ради которых они были предназначены. Должны быть разработаны методы и способы хранения биометрической информации, а так же средства по ее защите. Необходимо законодательно решить кто имеет право собирать, обрабатывать хранить информацию и кто будет ответственный за утечку данных.

Список литературы:

1. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) "О персональных данных" // Консультант Плюс URL: <https://goo.su/hlv12z> (дата обращения: 19.11.2022).
2. Половина россиян не поддержали создание властями биометрической системы // РБК URL: <https://goo.su/hDUEz> (дата обращения: 19.11.2022).
3. В правительстве назвали «основную миссию» по биометрии // РБК URL: <https://goo.su/3TFtLQJ> (дата обращения: 19.11.2022).
4. Компрометация тела, или как утекают биометрические данные // INFOWATCH URL: <https://goo.su/KwPQJ> (дата обращения: 19.11.2022).
5. Self-Service Food Kiosk Vendor Avanti Hacked // KREBSONSECURITY URL: <https://goo.su/4lhEz> (дата обращения: 19.11.2022).

6. Self-Service Food Kiosk Vendor Avanti Hacked // ehackingnews URL: <https://goo.su/IZShz31> (дата обращения: 19.11.2022).

7. Биометрия: риск утечки есть всегда // ИКС МЕДИА URL: <https://goo.su/zdKD6zI> (дата обращения: 19.11.2022).

8. Rs 500, 10 minutes, and you have access to billion Aadhaar details // The Tribune URL: <https://goo.su/TCPUWx> (дата обращения: 19.11.2022).

9. Используемая полицией биометрическая СКУД допустила утечку данных 1 млн человек // SecurityLab URL: <https://www.securitylab.ru/news/500471.php> (дата обращения: 19.11.2022).

10. Госдума заморозила законопроект по сбору биометрии в банках // CNEW URL: <https://goo.su/OtPWz1O> (дата обращения: 19.11.2022).