DOI: https://doi.org/10.15688/NBIT.jvolsu.2019.4.4

УДК 57.087.1
ББК 32.818

БИОМЕТРИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Герман Николаевич Чурилин

Студент кафедры информационной безопасности,
Волгоградский государственный университет
churilin.german@inbox.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Елена Александровна Максимова

Кандидат технических наук, доцент,
заведующая кафедрой информационной безопасности,
Волгоградский государственный университет
maksimova@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье рассматривается вопрос использования биометрических систем в информационных системах с точки зрения обеспечения информационной безопасности. Выделяются риски, которые могут повлиять на безопасность, и способы их минимизации.

Ключевые слова: биометрические системы, идентификация, аутентификация, биометрические персональные данные, информационная безопасность.

Для контроля доступа к информационным системам (ИС) далеко не последнюю роль играют процессы идентификации и аутентификации пользователей, которые позволяют определить пользователя по идентификатору и проверить его подлинность. И если в наиболее распространенном случае эти системы основаны на связке логин и пароль, т.е. пользователь должен запомнить эту комбинацию, то в последние годы возрастает популярность систем, использующих биометрические данные человека, которые всегда с нами и их невозможно забыть и потерять, что дает определенные удобства для пользователей, так как не требуется ничего запоминать или предъявлять каких-либо документов удостоверяющих личность. В данной статье речь пойдет о биометрических системах с точки зрения вопроса информационной безопасности, будут рассмотрены вопросы регулирования этого направления законодательством РФ, основные угрозы присущие этим системам и способы их минимизации.

Биометрические системы и принципы их функционирования основаны на науке о биометрии и биометрических данных. Под наукой о биометрии подразумеваются способы автоматизированного распознавания человека по уникальным физическим или/и психологическим признакам присущим только одному конкретному индивиду. Опираясь на межгосударственный стандарт [3], можно понять, что выделяют два ключевых понятия в данной сфере: биометрическую идентификацию (или по-другому

распознавание) и аутентификацию (она же верификация) и эти понятия, как может показаться на первый взгляд, далеко не одно и тоже [3]. Под биометрической идентификацией (распознаванием) понимается база данных, в которой хранятся все полученные образцы какого-либо признака всех индивидов, для которых требуется предоставить доступ, и при сравнении с каждым из которых можно определить является ли заявитель тем, чей признак есть в базе или нет. Биометрическая аутентификация (верификация) представляет собой сам процесс сравнения признака из БД с предъявляемым для подтверждения истинности и принятия соответствующего решения о предоставления доступа к ИС.

Биометрические данные можно разделить на три группы. Ниже представлена схема-классификация, на которой отображено деление на эти три группы и подвиды-представители технологий биометрии, которые относятся к этим группам (рис. 1). Под схемой дано краткое описание этих технологий:

Физиологические характеристики:

1) Отпечатки пальцев: теория об их уникальности была выдвинута еще в 1877 году. В наши дни этот признак является одним из самых распространенных и хорошо изученных, практически в каждом современном смартфоне есть датчик отпечатка пальца.

2) Геометрия кисти руки: для такого признака измеряется профиль руки, т.е. объем кисти и пальцев их длина, а также неровности ладони и расположение складок кожи на сгибах фаланг пальцев.

3) Радужная оболочка глаза: чтобы произвести распознавание используется видео захват с камеры с помощью программных средств выделяется область зрачка и самой радужной оболочки глаза. Далее полученное круговое изображение конвертируют в черно-белый прямоугольный формат iris code (подобие QR-кода).

4) Сетчатка глаза: метод основан на распознавании по уникальному рисунку сосудов и капилляров на сетчатке глаза. Сложен с технической точки зрения, может произойти отказ в распознавании в случае изменения рисунка от действия болезни или не правильном положении головы при сканировании.

5) Рисунок вен: бесконтактный способ распознавания, основан на способности гемоглобина крови поглощать инфракрасное излучение. В результате работы такого датчика, получают изображение, где рисунок вен выделен более темным цветом.

6) Лицо: данный вид технологии распознавания делится на два подвида: 2D и 3D распознавание. В основе двухмерного распознавания лежат плоские двухмерные изображения, лица на этих изображениях можно с помощью алгоритмов представить в виде графов со взвешенными вершинами и ребрами. Трехмерное распознавание представляет собой 3D сканирование лица с помощью специальных сканеров.

Психологические характеристики:

1) Почерк и анализ рукописной подписи: применяют теорию нейронных сетей. На сегодняшний день это одна из самых лучших технологий для распознавания графических

Рис. 1. Классификация средств биометрии

образов. Конкретно для этой задачи используют обучение нейронной сети с учителем [6].

2) Голос и ритм речи: голоса людей сильно отличаются и это обусловлено как физиологическими отличиями (в росте, весе, поле, возрасте, размере рта), так и психологическими (в громкости, скорости, высоте, в особенности дыхания). Современные системы распознавания учитывают все эти факторы, разбивают запись голоса на «голосовые отпечатки» и далее производят их оцифровку и сравнение.

3) Скорость и особенность печати на клавиатуре: основными отличительными характеристиками клавиатурного ввода является период удержания клавиши нажатой и время паузы между нажатиями клавиш. Этот метод сложно применить по отношению к малоопытным пользователям, т.к. их клавиатурный почерк еще недостаточно полностью сформирован. В случае обычного пользователя на эти характеристики может повлиять психологическое состояние (усталость, возбужденность или внешние отвлекающие факторы).

4) Походка: каждый человек передвигает свое тело в пространстве уникально, так как он не просто переставляет ноги, хотя их тоже можно переставлять по разному (например, человек может быть пожизненно хромым или переставлять ноги с разной скоростью), но и дополнительно совершает различные движения, одними из таких движений являются взмахи руками с разной интенсивностью. Это дает возможность для каждого индивида выделить паттерны-образцы походки и на их основе распознать человека.

К биохимическим характеристикам на данный момент времени можно отнести только один способ распознавания – ДНК (он же генетическая дактилоскопия). В любом биоматериале человека есть ДНК и по ее отличительным особенностям, выявляемым при анализе, можно однозначно определить индивида.

С каждым годом популярность технологий распознавания растет как на российском рынке, так и на зарубежном и в связи с тем, что не существует абсолютно неуязвимых технологий эта сфера входит в интересы специалистов по информационной безопасности. Согласно исследованиям J'son & Partners Consulting, основанным на опросе 15 ключевых вендоров и 26 интервью с крупными заказчиками, к 2020 году прогнозируется рост объема мирового рынка биометрического распознавания до $40 млрд [5] (рис. 2).

Уже сейчас практически все новые модели смартфонов и ноутбуков бизнес-класса оснащаются биометрическими датчиками. Например, в продукции Apple для массмаркета это технологии TouchID и FaceID, у Microsoft это WindowsHello. Если говорить о более серьезных отраслях таких как банки и бизнес системы, то биометрия начинает успешно внедряться и там. Например, начиная с лета 2018 года в России заработала Единая Биометрическая Система (далее ЕБС), оператором которой является «Ростелеком» и которая уже используется некоторыми крупными банками РФ [13].

Как уже сказано не существует систем, которые не могли бы быть полностью неуязвимыми. Одним из векторов защиты от нарушения информационной безопасности может является соблюдение законодательства ИБ в данной сфере. Первым делом стоит понимать, что биометрические признаки всех трех групп относятся к персональным данным (далее – ПД).

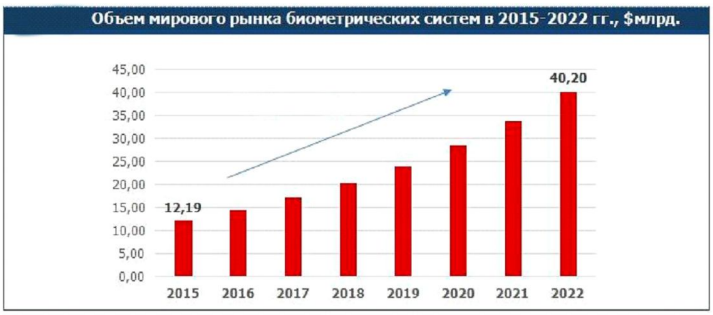

Рис. 2. Прогноз роста рынка биометрических технологий

Обратимся к федеральному закону № 152 «О персональных данных», в нем присутствует статья № 11, которая говорит нам о правилах обработки биометрии для операторов (первый пункт) только с письменного разрешения гражданина и для государства (второй пункт) во всех прочих случаях [11]. Отдельно выделенная статья № 14.1 в федеральном законе № 149 «Об информации, информационных технологиях и о защите информации» [12] также говорит о том, что обработка биометрических ПД возможна только с письменного согласия гражданина РФ, а помимо этого упоминается наличие отдельно созданного правительством федерального органа исполнительной власти для осуществления правового регулирования в сфере биометрической идентификации (ссылается на постановление правительства от 28 марта 2018 г. № 335). Этим органом является Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации и в его задачи входят следующие обязанности:

1) Определение порядка обработки, размещения биометрических ПД в ЕБС.

2) Разработка требований к методикам проверки при биометрической аутентификации.

3) Установление требований к информационным технологиям и аппаратным средствам, используемым при биометрическом распознавании/аутентификации в соответствии с приказом Минкомсвязи № 321 (приложение 3) [8].

4) Введение форм для документов, которые подтверждают соответствие какой-то конкретно информационной технологии или аппаратного средства требованиям, озвученным в пункте выше.

В свою очередь контроль и надзор за исполнением организационных и технических мер в организациях (кроме банковской сферы) возложен на ФСТЭК. Для банков этот контроль осуществляет ЦБ РФ. Продвигаясь, далее находим, что ближе к технической реализации имеют отношения два документа: ГОСТ Р ИСО/МЭК 19795-1–2007 и ГОСТ Р ИСО/МЭК 19784-1–2007 [1; 2]. Первый устанавливает требования к проведению эксплуатационных испытаний биометрических систем, второй описывает оптимальную обобщенную модель системы биометрического распознавания. Интересным фактом является то, что оба документа являются идентичными международным стандартам, т.е. являются переводами англоязычных версий ISO. Также следует выделить приказ ФСБ РФ от 16 декабря 2016 г. № 771, устанавливающий порядок получения, учета, использования биометрических ПД [9] и постановление Правительства РФ от 6 июля 2008 г. № 512 [7].

Однако даже при соблюдении всех рекомендаций и требований, выдвигаемых регуляторами и законодательством, не стоит упускать из виду вопрос надежности самих датчиков, используемых в системах распознавания для снятия биометрического образца. С надежностью датчиков связаны следующие вероятностные понятия:

1. Ошибки первого рода (FRR – False Rejection Rate) – вероятность ложного отказа пользователю для которого должен быть предоставлен доступ.

2. Ошибки второго рода (FAR – False Acceptance Rate) – вероятность ошибочного предоставления доступа злоумышленнику.

Отношение этих вероятностей показывает эффективность системы распознавания. Современные датчики и системы имеют низкие показатели возникновения ошибок и высокую скорость при распознавании, например, алгоритм ntechlab-003 российского вендора NTechLab, специализирующегося на системах машинного обучения, согласно исследованию 2017 года, проведенным NIST (National Institute of Standarts and Technology U.S.) был признан лучшим, показав отличные результаты на датасетах высокой сложности – «изображения сделанные в реальных условиях» и «фотографии детей» [16]. Но при всем при этом находятся способы обойти такого рода системы защиты и распознавания. Такие прецеденты, когда действительно удавалось экспериментально подтвердить возможность взлома, уже существуют. К примеру, согласно исследованиям [10] биометрические сканеры для распознавания по венам руки имеют довольно низкие вероятностные показатели ошибок (FAR = 0,0008 % и FRR = 0,01 %), но подобный сканер удалось обмануть, изготовив восковый слепок руки [14]. Вследствие этого стоит рассмотреть какие существуют риски нарушения ИБ при использовании биометрических систем и существующие рекомендации по их предотвращению.

В общем случае можно выделить следующие типы рисков:

1) Риски, которые могут возникать при сборе биометрических данных. Такими рисками являются угроза нарушения целостности в случае подмены или удаления биометрических ПД сотрудниками, занимающимися сбором этих образцов и занесением их в систему, угроза нарушения конфиденциальности в случае раскрытия, передачи образцов третьим лицам.

2) Риски, которые связанные с нарушениями при неправильной обработке/хранении биометрических ПД. Сюда, например, можно отнести хранение подобных данных в незашифрованном виде на носителях данных, не соответствующих требуемым степеням защищенности и такие прецеденты уже есть [15].

3) Риски, которые могут возникать в ходе процесса биометрической верификации в случае успешной подделки злоумышленником образцов биометрического материала.

Для предотвращения таких рисков, рассмотрим рекомендации, которые дает ЦБ РФ в следствии введения системы Единой Биометрической Системы (ЕБС) [4]:

1) Рекомендуется использовать средства криптографической защиты информации (СЗКИ), имеющие подтверждение требований надежности. Этот пункт может относится к минимизации второго риска.

2) Рекомендуется размещать объекты, связанные с обработкой биометрических ПД в отдельных сегментах вычислительных сетей. Доступ к отдельному сегменту проще контролировать, а значит лица, не имеющие на то доступ, легко его не получат. Этот пункт минимизирует первый риск.

3) Рекомендуется уведомить сотрудника, занимающегося обработкой и сбором биометрических данных, о протоколировании его действий и об ответственности за нарушение законодательства РФ в данной сфере. Данный пункт также минимизирует первый риск.

4) Рекомендуется исключить возможность хранения биометрических персональных данных физических лиц на рабочем месте, предназначенном для сбора/обработки биометрических ПД, после завершения регистрации биометрических ПД. Это минимизирует третий риск, так как один из каналов, для утечки образцов с целью их подделки, будет закрыт.

5) Использовать средства электронной цифровой подписи (ЭЦП) для гарантии контроля целостности собираемых биометрических данных.

Таким образом, в заключении статьи необходимо отметить, что биометрические системы однозначно могут являться более удобными системами идентификации пользователей, но на данный момент времени нет однозначных доводов в пользу того, что эти системы являются более надежными, чем «традиционные», к тому же для хранения биометрических образцов требуется обеспечивать крайне высокий уровень защиты, особенно это касается банковского и бизнес сектора, в котором активно начали внедрять эти технологии.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 19784-1-2007. – Электрон. текстовые дан. – Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-19784-1-2007 (дата обращения: 07.11.2019). – Загл. с экрана.

2. ГОСТ Р ИСО/МЭК 19795-1-2007. – Электрон. текстовые дан. – Режим доступа: http://docs.cntd.ru/document/1200067413 (дата обращения: 07.11.2019). – Загл. с экрана.

3. ГОСТ ISO/IEC 2382-37-2016 Информационные технологии (ИТ). Словарь. Часть 37. Биометрия. – Электрон. текстовые дан. – Режим доступа: http://docs.cntd.ru/document/1200144206 (дата обращения: 23.10.2019). – Загл. с экрана.

4. Методические рекомендации по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации. – Электрон. текстовые дан. – Режим доступа: http://www.cbr.ru/content/document/file/62907/4mr.pdf (дата обращения: 07.11.2019). – Загл. с экрана.

5. Мировой рынок биометрических систем, 2015–2022 гг. – Электрон. текстовые дан. – Режим доступа: http://json.tv/ict_telecom_analytics_view/mirovoy-rynok-biometricheskih-sistem-2015-2022-gg-20170119025618 (дата обращения: 23.10.2019). – Загл. с экрана.

6. Обучение нейросети с учителем, без учителя, с подкреплением – в чем отличие? Какой алгоритм лучше? – Электрон. текстовые дан. – Режим доступа: https://neurohive.io/ru/osnovy-data-science/obuchenie-s-uchitelem-bez-uchitelja-s-

podkrepleniem (дата обращения: 23.10.2019). – Загл. с экрана.

7. Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных». – Доступ из информ.-правового портала «Гарант.ру».

8. Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 25.06.2018 № 321. – Доступ из информ.-правового портала «Гарант.ру».

9. Приказ Федеральной службы безопасности Российской Федерации от 16.12.2016 № 771. – Электрон. текстовые дан. – Режим доступа: https://rg.ru/2017/02/10/persondan-dok.html (дата обращения: 07.11.2019). – Загл. с экрана.

10. Сабанов, А. Г. Сравнительный анализ методов биометрической идентификации личности / А. Г. Сабанов, С. Г. Смолина. – М. : Труды ИСА РАН, 2016. – Т. 66. – С. 11–20.

11. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 31.12.2017). – Доступ из справ.-правовой системы «КонсультантПлюс».

12. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс».

13. ЦБ решил обязать банки оказывать услуги с использованием биометрии клиентов. – Электрон. текстовые дан. – Режим доступа: https://www.interfax.ru/business/662298 (дата обращения: 07.11.2019). – Загл. с экрана.

14. Эксперты нашли способ обхода биометрической аутентификации по сосудам. – Электрон. текстовые дан. – Режим доступа: https://www.securitylab.ru/news/497290.php (дата обращения: 23.10.2019). – Загл. с экрана.

15. Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms. – Electronic text data. – Mode of access: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms (accessed 23 October 2019).

16. The 2017 IARPA Face Recognition Prize Challenge (FRPC). – Electronic text data. – Mode of access: https://www.nist.gov/sites/default/files/documents/2017/11/22/nistir_8197.pdf (accessed 23 October 2019).

REFERENCES

1. *GOST R ISO/MEK 19784-1-2007* [GOST P ИСО/МЭК 19784-1-2007]. URL: http://docs.cntd.ru/document/gost-r-iso-mek-19784-1-2007 (accessed 7 November 2019).

2. *GOST R ISO/MEK 19795-1-2007* [GOST P ИСО/МЭК 19795-1-2007]. URL: http://docs.cntd.ru/document/1200067413 (accessed 7 November 2019).

3. *GOST ISO/IEC 2382-37-2016 Informatsionnye tekhnologii (IT). Slovar. Chast 37. Biometriya* [GOST ISO/IEC 2382-37-2016 Information Technology (IT). Dictionary. Part 37. Biometrics]. URL: http://docs.cntd.ru/document/1200144206 (accessed 23 October 2019).

4. *Metodicheskie rekomendatsii po neytralizatsii bankami ugroz bezopasnosti, aktualnykh pri obrabotke, vklyuchaya sbor i khranenie, biometricheskikh personalnykh dannykh, ikh proverke i peredache informatsii o stepeni ikh sootvetstviya predostavlennym biometricheskim personalnym dannym grazhdanina Rossiyskoy Federatsii* [Guidelines for Banks to Neutralize Security Threats That Are Relevant in the Processing, Including Collection and Storage, of Biometric Personal Data, Their Verification and Transmission of Information About the Degree of Their Compliance with the Provided Biometric Personal Data of a Citizen of the Russian Federation]. URL: http://www.cbr.ru/content/document/file/62907/4mr.pdf (accessed 7 November 2019).

5. *Mirovoy rynok biometricheskikh sistem, 2015–2022 gg.* [Global Biometric Systems Market 2015–2022]. URL: http://json.tv/ict_telecom_analytics_view/mirovoy-rynok-biometricheskih-sistem-2015-2022-gg-20170119025618 (accessed 23 October 2019).

6. *Obuchenie neyroseti s uchitelem, bez uchitelya, s podkrepleniem – v chem otlichie? Kakoy algoritm luchshe?* [Neural Network Training with a Teacher, Without a Teacher, with Reinforcement – What is the Difference? Which Algorithm is Better?]. URL: https://neurohive.io/ru/osnovy-data-science/obuchenie-s-uchitelem-bez-uchitelja-s-podkrepleniem/ (accessed 23 October 2019).

7. *Postanovlenie Pravitelstva RF ot 06.07.2008 № 512 «Ob utverzhdenii trebovaniy k materialnym nositelyam biometricheskikh personalnykh dannykh i tekhnologiyam khraneniya takikh dannykh vne informatsionnykh sistem personalnykh dannykh»* [Resolution of the Government of the Russian Federation of July 6, 2008 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"]. Access from "Garant" Informational and Legal Web Portal.

8. *Prikaz Ministerstva tsifrovogo razvitiya, svyazi i massovykh kommunikatsiy RF ot 25.06.2018 № 321* [Order of the Ministry of Digital Development, Communications and Mass Communications of the Russian Federation of June 25, 2018, no. 321]. Access from "Garant" Informational and Legal Web Portal.

9. *Prikaz Federalnoy sluzhby bezopasnosti Rossiyskoy Federatsii ot 16.12.2016 № 771* [Order of the Federal Security Service of the Russian Federation of December 16, 2016 no. 771]. URL: https://rg.ru/2017/02/10/persondan-dok.html (accessed 07 November 2019).

10. Sabanov A.G., Smolina S.G. *Sravnitelnyy analiz metodov biometricheskoy identifikatsii lichnosti* [Comparative Analysis of Biometric Identification Methods]. Moscow, Trudy ISA RAN, 2016, vol. 66, pp. 11-20.

11. *Federalnyy zakon ot 27.07.2006 № 152-FZ «O personalnykh dannykh» (red. ot 31.12.2017)* [Federal Law of July 27, 2006 no. 152-FZ "On Personal Data" as Amended on December 31, 2017]. Access from Reference Legal System "KonsultantPlus".

12. *Federalnyy zakon «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» ot 27.07.2006 № 149-FZ* [Federal Law "On Information, Information Technologies and Information Protection" of July 27, 2006 no. 149-FZ]. Access from Reference Legal System "KonsultantPlus".

13. *TSB reshil obyazat banki okazyvat uslugi s ispolzovaniem biometrii klientov* [Central Bank Decided to Oblige Banks to Provide Services Using Customer Biometrics]. URL: https://www.interfax.ru/business/662298 (accessed 7 November 2019).

14. *Eksperty nashli sposob obkhoda biometricheskoy autentifikatsii po sosudam* [Experts Have Found a Way to Bypass Biometric Authentication by Vessels]. URL: https://www.securitylab.ru/news/497290.php (accessed 23 October 2019).

15. *Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms*. URL: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms (accessed 23 October 2019).

16. *The 2017 IARPA Face Recognition Prize Challenge (FRPC)*. URL: https://www.nist.gov/sites/default/files/documents/2017/11/22/nistir_8197.pdf (accessed 23 October 2019).

BIOMETRICS IN INFORMATION SECURITY

German N. Churilin

Student, Department of Information Security,
Volgograd State University
churilin.german@inbox.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Elena A. Maksimova

Candidate of Sciences (Engineering), Associate Professor,
Head of the Department of Information Security,
Volgograd State University
maksimova@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. To control the access to information systems (IS), user identification and authentication processes play an important role, which allows to identify the user by the identifier and verify its authenticity. In the most common case, these systems are based on a combination of a username and a password, i.e. the user must remember this combination. However, in recent years, the popularity of systems that use human biometric data, which is always with us and can not be forgotten or lost, has increased, which provides certain convenience for users, since they do not need to remember anything or present any identity documents. This article focuses on biometric systems from the point of view of information security. The paper addresses the issues of regulating this area by the legislation of the Russian Federation, the main threats inherent in these systems and ways to minimize them. The article discusses the use of biometric recognition in information systems as part of information security. The authors highlight the risks that may affect security and means to minimize them.

Key words: biometric recognition system, identification, authentication, biometric personal data, information security.