Ю. С. Селезнева, В. Г. Пуртов
Тюменский государственный университет, г. Тюмень
УДК 004.056.5

БИОМЕТРИЧЕСКАЯ СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ В МАЛЫХ МЕДИЦИНСКИХ УЧРЕЖДЕНИЯХ

Аннотация. В работе рассмотрены преимущества и проблемы реализации биометрических систем в малых медицинских учреждениях, правовые и этические последствия использования биометрических систем, включая вопросы конфиденциальности и защиты данных. Также анализируется потенциальное влияние биометрических систем на общее качество медицинских услуг.

Ключевые слова: биометрическая система, медицинские учреждения, информационная безопасность, конфиденциальные данные, защита данных.

Введение. В последние годы растет обеспокоенность по поводу безопасности конфиденциальной информации в медицинских учреждениях [1]. С ростом количества утечек данных и кибератак, для медицинских учреждений стало важным внедрение эффективных мер безопасности для защиты информации о пациентах. Одним из таких способов является использование биометрических систем для управления и контроля доступа [2].

Биометрические системы основаны на уникальных характеристиках человека. Такими идентификаторами могут быть отпечатки пальцев, распознавание лица, голоса, радужной оболочки и другие. Биометрические системы широко используются в банках, промышленности, медицине и других областях, и их эффективность в целях повышения безопасности доказана в научных работах О. И. Долгановой, Д. А. Чистяковой, Е. С. Багаева и Н. И. Мазниченко [3-5].

Исследования, проводимые в области защиты персональных данных пациентов и работников медицинских учреждений при помощи биометрических систем основываются на общепринятых стандартах и не учитывают особенностей организации управления и контроля доступа в малых медицинских учреждениях. Такие организации имеют ограниченный бюджет и особую степень внедрения информационных технологий.

Небольшие медицинские учреждения, такие как клиники и частные практики, особенно уязвимы из-за их ограниченных ресурсов и отсутствия опыта в применении мер безопасности. Тем не менее, эти учреждения также обрабатывают конфиденциальную информацию о пациентах, и нарушение установленных правил может иметь серьезные последствия как для пациентов, так и для самой организации.

Объектом исследований в работе «Биометрическая система контроля и управления доступом в малых медицинских учреждениях» является реализация и внедрение биометрической системы для контроля и управления доступом в медицинских учреждениях. Предметом исследования являются малые медицинские учреждения.

Проблема исследования. В научной работе производится попытка внести вклад в раздел информационной безопасности в области медицины. Исследование направлено на то, чтобы дать представление о том какие преимущества дает внедрение биометрической системы в малых медицинских учреждениях и с какими проблемами при этом можно столкнуться. Задачей данной работы является выявление и оценка достоинств и проблем реализации биометрической системы для контроля доступа в малых медицинских учреждениях, включая влияние на безопасность, удобство и экономическую эффективность.

Материалы и методы. Вероятность возникновения ошибок в биометрической системе контроля доступа определяется двумя параметрами: FAR (False Acceptance Rate) — коэффициент несанкционированного допуска (ошибка первого рода), когда система предоставляет доступ незарегистрированному пользователю и FRR (False Rejection Rate) — система не предоставляет доступ зарегистрированному пользователю (ошибка второго рода).

Такие системы используют комбинацию аппаратного и программного обеспечения для сбора, обработки и хранения биометрических данных. К аппаратным компонентам можно отнести датчики, сканеры, камеры или другие устройства, собирающие биометрию человека. Устройства контроля доступа необходимо располагать в помещении так, чтобы работа с биометрической системой была удобной и безопасной. Также стоит учитывать положение естественного

и искусственного освещения. Самыми широко используемыми являются сканеры отпечатков пальцев, их существует большее количества из-за доступности самой технологии идентификации по отпечатку пальца. Стоимость таких сканеров варьируется от 4 тыс. до 720 тыс. рублей. Самым дорогостоящим оборудованием являются сканеры сетчатки глаза. Ценовой диапазон таких считывателей 30 тыс. — 5 млн рублей. Все устройства, использующиеся в медицинском учреждении для контроля доступа с помощью биометрической системы, должны быть сертифицированы и соответствовать ГОСТу ISO/IEC 19794-1-2015 [9].

Программные компоненты включают в себя алгоритмы, обрабатывающие и сравнивающие данные с базой данных зарегистрированных пользователей. Рассмотрим четыре вида биометрических особенностей человека (лицо, голос, отпечаток пальца и сетчатка глаза), которые применяются для контроля доступа в системах, а также требования, которым они должны соответствовать.

При идентификации по форме лица используются компьютерные программы, которые анализируют изображение лица и проверяют такие характеристики, как расстояние между оптическими центрами зрачков, угол челюсти, длина носа, в результате чего создается уникальный шаблон. Далее программа сравнивает данный шаблон с уже имеющимися изображениями и оценивает, насколько они схожи.

При идентификации по отпечатку пальца используется уникальный рисунок папиллярных узоров на пальцах человека, который считывается при помощи сканера и в оцифрованном виде хранится в базе данных. Это самый распространенный метод контроля доступа в биометрических системах.

При идентификации по голосу используются шаблоны записи голоса: конкретная фраза продолжительностью от 5 секунд или произвольный набор слов, который длится не менее 16 секунд. Сравнение происходит по резонансным отклонениям в спектре голоса, что делает этот метод контроля доступа устойчивым к внешним шумам и помогает анализировать состояние человека для выявления его физического и эмоционального состояния.

При идентификации по сетчатке глаза используется уникальный рисунок кровеносных сосудов глазного дна с помощью инфракрасного излучения низкой интенсивности, которое направляется к задней стенке глаза через зрачок. Данный метод контроля доступа имеет большое количество требований. Человек должен находиться достаточно близко к сканеру (не дальше 7 см) и быть абсолютно неподвижным. Точность полученного изображения во многом зависит от внешнего освещения вокруг человека, которое влияет на размер зрачка, ведь при его малом размере будет уменьшено количество света, попадающего на сетчатку. В связи с этими особенностями идентификация по сетчатке глаза является более надежным методом защиты, чем предыдущие из-за сложности рисунка и того, что сетчатка глаза практически неизменна в течение всей жизни человека, если не брать во внимание перенесенные болезни или полученные травмы, в результате которых сетчатка может измениться.

Обеспечение защиты обработки медицинских биометрических данных должно проводиться в соответствии с действующим законодательством Российской Федерации. Рассмотрим особенности использования биометрических систем. Медицинское учреждение относится к субъектам малого предпринимательства, если средняя численность персонала за предыдущий календарный год не более ста человек включительно [6]. Согласие пациента — обязательное условие при сборе информации. Обязательным требованием медицинского вмешательства является информированное добровольное согласие человека [7]. Если организация идентифицируется как ИП, то она не может обрабатывать, хранить и собирать биометрические данные, если они не будут занесены в Единую биометрическую систему [8].

Таким образом, разработка обязательной документации и требований по защите данных пациентов и работников организации является важным и трудоемким этапом при обеспечении безопасности данных в малых медицинских учреждениях.

Результаты. С целью выявления и оценки преимуществ и проблем реализации биометрической системы для контроля доступа в

малых медицинских учреждениях был проведен анализ научных работ на данную тему, изучены вышеперечисленные особенности биометрических систем и их основные принципы, в результате чего были получены следующие выводы.

Биометрические системы позволяют медицинским организациям осуществлять контроль доступа, что помогает предотвратить несанкционированный доступ и кражу данных. Биометрические системы могут использоваться для отслеживания посещаемости сотрудников и медицинских работников, что в результате повысит производительность. Биометрические системы более точны и безопасны, чем традиционные методы аутентификации, такие как, например, пароли. Они могут помочь уменьшить ошибки в системе и повысить безопасность пациентов, поскольку они основаны на уникальных физиологических или поведенческих характеристиках, которые не могут быть легко воспроизведены.

Для того чтобы использовать биометрические системы в малых медицинских учреждениях необходимо согласие пациента, которое является обязательным условием при сборе данных. Оборудование и программное обеспечение, использующиеся для контроля и управления доступом с помощью биометрической системы, должны быть сертифицированы и соответствовать ГОСТу ISO/IEC 19794-1-2015. Документация, необходимая для использования и внедрения биометрических систем в учреждении, должна быть тщательно разработана и соответствовать законодательству Российской Федерации.

Использование биометрических систем может быть затруднительно из-за технических проблем, таких как сбои датчиков и сбои программного обеспечения, которые могут привести к сбоям аутентификации. Биометрические системы могут быть дорогими в реализации, особенно для малых медицинских учреждений с ограниченным бюджетом, ведь для проведения соответствующих мероприятий необходимо надлежащее оборудование и выделенные средства для внедрения этой системы в организацию. Биометрические системы могут быть доступны не всем пользователям, особенно тем, кому неудобен или невозможен способ сбора и хранения их биометрических данных. Также необходимо выделить возможность изменения

биометрических данных в результате аварии, болезни или других факторов, влияющих на биометрию человека.

Заключение. Применение биометрических систем для контроля и управления доступом в малых медицинских учреждениях является эффективной мерой для повышения безопасности и улучшения системы здравоохранения. Реализация биометрических систем может обеспечить точную идентификацию людей, предотвратить несанкционированный доступ и защитить конфиденциальную информацию пациентов. Однако, реализацию биометрических систем следует тщательно рассмотреть с учетом юридических и этических последствий. Малые медицинские учреждения должны оценить различные типы доступных биометрических систем и выбрать тот, который наилучшим образом соответствует их потребностям и ресурсам. Необходимо выявить слабые места системы, чтобы избежать нарушения личных прав и свобод человека, на что в дальнейшем будут направлены мои будущие работы. Таким образом, в настоящее время актуальной задачей является повышение доступности использования биометрических систем контроля доступа для малых медицинских учреждений.

СПИСОК ЛИТЕРАТУРЫ

1. Салимова Г. Х. С. Био-и информационные технологии, и биометрия в контексте персональных данных / Салимова Г. Х. С., Попова А. В. — Текст: непосредственный // E-Scio. — 2021. — №. 4 (55). — С. 353-360.
2. Зыков В. Д. Обеспечение защиты информации при обработке медицинских биометрических данных / В.Д. Зыков, Р.В. Мещеряков, А.С. Романов, А.А. Шелупанов — Текст: непосредственный // Доклады Томского государственного университета систем управления и радиоэлектроники. — 2010. — №. 2-2 (22). — С. 249-252.
3. Багаев Е. С. Современные биометрические системы безопасности / Багаев Е. С. — Текст: непосредственный // Вестник магистратуры. — 2014. — №. 6-1 (33). — С. 21-26.
4. Долганова О. И. Варианты использования Единой биометрической системы как инструмента доступа к цифровому профилю гражданина / Долганова О. И., Чистякова Д. А. — Текст: непосредственный // Государственное управление. Электронный вестник. — 2022. — №. 93. — С. 134-149.

5. Мазниченко Н. И. Области применения и принципы построения биометрических систем идентификации личности / Мазниченко Н. И. — Текст: непосредственный //Вестник Национального технического университета Харьковский политехнический институт. Серия: Информатика и моделирование. — 2007. — №. 19. — С. 127-132.
6. Федеральный закон от 24.07.2007 № 209-ФЗ (последняя редакция) «О развитии малого и среднего предпринимательства в Российской Федерации» // Собрание законодательства Российской Федерации. — 2007.
7. Федеральный закон от 21.11. 2011 N 323-ФЗ (ред. от 03.07. 2016) «Об основах охраны здоровья граждан в Российской Федерации» (с изм. и доп., вступ. в силу с 01.01.2017) // Собрание законодательства Российской Федерации. — 2014. — №. 519-ФЗ.
8. Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации»: принят Государственной Думой 21 декабря 2022 года : одобрен Советом Федерации 23 декабря 2022 года // Собрание законодательства Российской Федерации. — 2022.
9. ГОСТ ISO/IEC 19794-1-2015 Информационные технологии (ИТ). Биометрия. Форматы обмена биометрическими данными: утвержден и введен в действие в качестве национального стандарта Российской Федерации с 1 июля 2016 г.