УДК 004.04

СОВРЕМЕННЫЕ БИОМЕТРИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Айтжанов Серик Дуйсенбаевич
Serik5555557@gmail.com
Магистрант кафедры «Радиотехника, электроника и телекоммуникации» ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Н.М. Казиева

Применению биометрических данных нет границ. В цифровом мире многие из нас ежедневно используют «умные» цифровые устройства для выполнения рутинных задач. В тенденции роста количества «умных» цифровых устройств по всему миру пропорционально растет и число случаев краж и утечек персональных данных от злоумышленников. Отсюда возникает вопрос о повышении потребности в создании новых и модернизации существующих способов защиты информации. Одним из существующих на текущий момент способов являются биометрические системы безопасности. Защита информации на основе биометрических данных позволяет предоставить надежную защиту данных на основе измерений и анализе уникальных присущие только этому человеку физических характеристик. Этот способ широко применяется как для защиты отдельных лиц, так и для защиты всех типов предприятий и организаций.

Биометрия позволяет проводить идентификацию и аутентификацию человека на основе узнаваемых и поддающихся проверке уникальных данных. При биометрической аутентификации проводится сравнение полученных данных о характеристиках человека с биометрическим «шаблоном» данного человека для определения сходства. Первоначально «шаблон» необходимо сохранить в базу данных. Сохраненные данные применяются в сравнении с полученными биометрическими данными человека для аутентификации [1].

Биометрическая идентификация подразумевает установление личности человека. Суть состоит в захвате элемента биометрических данных от этого человека. Под этим понимают изображение их лица, запись голоса либо изображение их отпечатков пальцев. Далее при запросе доступа данные, полученные от специальных устройств-считывателей, приводят в сравнение с биометрическими данными нескольких других лиц, которые хранятся в базе данных.

На данный момент биометрические системы подразделяются физиологическую и поведенческую биометрию. Каждый из типов имеют собственные особенности. К физиологической биометрии относят сканирование, анализ и преобразование в цифровой формат биометрических данных человека специальными датчиками и считывателями. К биометрическим данным относятся радужная оболочка и сетчатка глаза, отпечатки пальцев, изображения вен, формы лица, руки, пальцев и многие другие. При поведенческой биометрии оцениваются уникальные динамические или поведенческие характеристики человека. В эти характеристики входят динамика почерка, подписи, нажатия клавиш и определение скорости набора текста в момент эксплуатации электронных средств, голосовой и речевой ритм,

походка, звук шагов, распознавание жестов, использование предметов. На рисунок 1 изображены примеры физиологических и поведенческих измерений.

Рисунок 1 - Примеры физиологических и поведенческих измерений [2].

Исходя из этого, следует, что необходимо исследовать и развивать биометрические методы идентификации и защиты информации для обеспечения должной защиты конфиденциальных данных. Далее мы рассмотрим биометрические методы, которые существуют на сегодняшний день с их преимуществами и недостатками. Первым рассмотрим распознавание по отпечатку пальцев. В этом методе используется сканер отпечатков пальцев. Чаще всего можно выделить три типа: преобразование отпечатка пальца в цифровой код с помощью оптического датчика, сохранение преобразования с помощью линейного термодатчика и преобразование отпечатка пальца с помощью емкостного датчика. Разница для конечного пользователя будет заключаться в манипуляции со сканером. Плюсом этого метода являются уникальные идентификаторы отпечатка пальцев каждого человека, широко известен данный метод аутентификации, отсутствие необходимости в запоминании сложных паролей, а также дешевизна и доступность сканеров отпечатков пальцев. Минусом сканирования отпечатков пальцев считается временные и постоянные травмы, которые могут препятствовать сканированию. Возможен обход с помощью методов, копирующих и воспроизводящих отпечатки пальцев [3].

Далее рассмотрим распознавание голоса. Интеграция этой технологии ускоряет процесс обслуживания, уменьшает нагрузку агентам и повышает их точность и результативность. Эта технология имеет широкие варианты его использования, такие как системы безопасности, проверка кредитных карт, телеконференции, анализ в криминалистике, и другие. При необходимости высокой защиты конфиденциальных данных, возможно объединение и использование совместно с другим методом аутентификации. Плюсами этого метода являются отсутствие необходимости запоминания и использования пароля, уменьшение времени на процесс обработки пользователей агентами, особенно при эксплуатации пассивной голосовой биометрии и сложности подделки голоса. Минусом этого метода являются сложность успешной аутентификации в шумных местах.

Следующий метод – это распознавание радужной оболочки глаза. На текущий момент, данный метод биометрической аутентификации один из самых точных и осуществляется благодаря специальным сканерам радужной оболочки глаза. Первым этапом в этой технологии является определение местонахождения зрачка. Далее идет процесс нахождения радужной оболочки и век. После этого, веки и ресницы исключаются как ненужные части. Остается радужная оболочка, которую разделяют по блокам и их преобразуют в числовые значения, строящие изображение. В итоге, соответствие с ранее собранными данными осуществляется с применением тех же методов проверки личности. Данная технология

является относительно новой и требует доработки, при низкой освещенности распознавание радужной оболочки малы.

Мы подошли к следующему методу — распознавание лица. Данная технология используют уникальную анатомию и черты лица человека для идентификации человека по имеющимся данным — изображениям лица, хранящегося в базе данных в виде математического кода. Метод довольно популярен по причине применения его в видеоконференцсвязи. Распознавание лица не требует большого взаимодействия с устройством, широко применим, и дает при интеграции с другими биометрическими методами высокую эффективность работы. Но на производительность системы влияет изменение освещения. При использовании аксессуаров может усложнить верификацию пользователя.

Перейдем к следующему методу, к распознаванию рукописного ввода. Динамическая проверка подписи используется в тех видах деятельности, которые требуют обеспечение автономной работы рабочих процессов на примере банковских и судебных систем. Основой идентификации подписи является алгоритмы распознавания образов либо математических методов анализа кривых, так как набор точек может быть подпись. Исходя из этого, в данных системах чаще всего применяют декомпозицию временных рядов или аппроксимацию кривой. Данной технологии нет необходимости в сложных системах для полноценной работы. Однако метод подходит только операций низкого уровня безопасности [4].

Следующие два метода биометрической аутентификации, которые будут описаны далее, не так широко распространены, но в ближайшем будущем получат свою долю внимания. Первым представителем является распознавание походки. Данная технология применяет для идентификации манеру походки. Ходьба каждого человека имеет собственные особенности. К примеру, можно описать каким образом ставится одна нога перед другой. Тем самым, это является эффективным способом идентификации личности человека. Все больше и больше становится популярным формат непрерывной аутентификации. Исходит от того, метод непрерывной аутентификации будет обеспечивать лучший пользовательский опыт. Помимо этого, что пользователи вместо паролей больше предпочитают использовать системы биометрической аутентификации.

И вторым методом является метод распознавание вен. Метод основывается на эксплуатации уникального изображения кровеносных сосудов на руке человека для определения личности человека. При получения изображения используется инфракрасный свет для картирования вен под кожей на руках или пальцах. Метод имеет высокий уровень точности. Распознавание вен один из самых продвинутых систем биометрической идентификации на текущий момент [5].

Таким образом, в рамках этой статьи рассмотрены методы биометрической защиты, выполнен анализ преимуществ и недостаток этих методов. Результаты анализа могут быть использованы для дальнейшего исследования в рамках биометрической идентификации личности человека в различных объектах, где это представляется необходимым.

Список использованной литературы

1. Кухарев Г.А. Биометрические системы: Методы и средства идентификации личности человека. СПб.: Политехника, 2001. 97 с.

2. Урбах В.Ю. Биометрические методы. М.: Наука, 1964. 416 с.

3. Краковский Ю. М. Методы защиты информации. Учебное пособие для вузов / Ю. М. Краковский. - 3-е изд., перераб. СПб, Лань, 2021. 236 с.

4. Грижебовская А. Г., Михалев А. В. Биометрический метод идентификации человека по сосудистому рисунку пальца. Вопросы кибербезопасности, № 5 (33), 2019, 56 с.

5. https://www.thalesgroup.com/en/markets/digital-identity-andsecurity/government/inspired/biometrics