УДК 340

ПРАВОВЫЕ СРЕДСТВА, МЕТОДЫ И СОВРЕМЕННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ НА МЕЖДУНАРОДНОМ УРОВНЕ ПО БОРЬБЕ С ТЕРРОРИЗМОМ С ПОМОЩЬЮ БИОМЕТРИЧЕСКИХ СИСТЕМ И БАЗ ДАННЫХ

К.А. ГАЙКОВА
(Представлено: А.С. ВАЛЕВКО)

В публикации рассматриваются правовые средства, методы и современные технологии, используемые на международном уровне по борьбе с терроризмом с помощь биометрических систем и баз данных.

За последнее время было проведено множество исследований в таких разнообразных областях, как: биометрии, биологии, биоинженерии, биохимии, медицины и других не менее важных секциях. В результате таких исследований был получен вывод о том, что биометрические технологии достигли достаточно высокого уровня, который может удовлетворить потребности не только правоохранительных органов, но и международных организаций, на примере Интерпола. Как и ко всем видам персональных данных, к биометрическим, есть нормативно-правовые требования на международном уровне, которые предусматривают определенные рамки по использованию биометрии, дабы избежать нарушений в области прав человека и прав на неприкосновенность частной жизни.

В соответствии с Резолюцией 1624 (2005) Совета Безопасности ООН, предусматривается, что государства обязаны защищать лиц, находящихся в их юрисдикции, от террористических атак и привлекать виновных в совершении подобных деяний к ответственности, обеспечивая при этом соблюдение прав человека. Уважение прав человека и принципа верховенства закона связано с эффективной контртеррористической деятельностью и является необходимым условием успешной борьбы с терроризмом [3].

В соответствии с Резолюцией 2396 Совет Безопасности ООН призывает государства-члены проводить проверку и расследования в отношении подозреваемых иностранных боевиков-террористов и сопровождающих их членов семьи, в том числе их супругов и детей, а также разрабатывать процедуры и проводить всеобъемлющие оценки рисков в отношении этих лиц [4]. Также при разработке систем по сбору биометрических персональных данных важно учитывать гарантии в отношении защиты данных и соблюдения стандартов прав человека.

На данный момент могут использоваться следующие виды идентификации личности:

1) химический;
2) визуальный;
3) визуально-пространственный;
4) поведенческий;
5) обонятельный;
6) распознавание вен;
7) слуховой.

Химический способ представляет собой соотнесение ДНК (дезоксирибонуклеиновая кислота), то есть идентификация производится с помощью анализа отдельных частей ДНК.

Визуальный способ распознавания личности включает в себя:

1) аунтефикацию личности путем сравнения ушной раковины человека;
2) использование особенностей, обнаруженных в радужной оболочке для идентификации личности;
3) использование рисунков вен в задней части глаза для достижения распознавания;
4) дактилоскопия (идентификация человека по отпечаткам пальцев рук) также относится к визуальному способу.

Исходя из названия визуально-пространственного способа распознавания личности можно сделать вывод, что в рассматриваемом методе будут использоваться 3D модели. Такие макеты применяются для воссоздания геометрии пальцев и рук, также данная технология может применяться и для геометрии лица человека.

Поведенческий метод подразумевает особенности поведения личности, то есть сюда можно отнести:

1) распознавание по походке – использование индивидуального стиля ходьбы или походки для определения личности;
2) распознавание ввода – использование уникальных характеристик типирования лиц для установления личности;
3) распознавание подписи – аутентификация личности осуществляется путем анализа стиля почерка, в частности подписи. Существует два основных типа идентификации цифровой или рукописной подписи: статическая и динамическая. Статическая чаще всего представляет собой визуальное сравнение между одной сканированной подписью с другой или сканированной подписью и рукописной. Технология

доступна для проверки двух сканированных сигнатур с использованием передовых инноваций. Динамика же становится все более популярной, в связи с использованием специально-предназначенного для этого оборудования. Подобные данные могут быть использованы в суде для создания биометрического шаблона, из которого динамические подписи могут быть аутентифицированы либо в момент подписания, либо после подписания. Такое быстрое реагирование поспособствует для обнаружения недобросовестного использования чужих подписей.

Следующий ранее указанный метод идентификации – обонятельный, использующий особенности индивидуального запаха для определения личности.

Распознавание вен – это тип биометрии, который может быть использован для идентификации людей на основе рисунков вен в человеческом пальце или ладони.

Последним приведенным выше способом является слуховой, включающий в себя:

Идентификация голоса – это соответствие исходного голоса с предоставленным шаблоном. Системы идентификации также могут быть реализованы скрытно без ведома пользователя для более точного распознавания говорящих в дискуссии. В криминалистических приложениях обычно сначала выполняют процесс идентификации говорящего, чтобы создать список «лучших соответствий», а затем выполняют ряд процессов проверки для определения окончательного соответствия.

Аутентификация Голоса – это использование уже заранее записанного голоса для контроля доступа, то есть процедура проверки подлинности голоса. Голос говорящего должен соответствовать заранее записанному шаблону, так называемой «голосовой печатью» или «голосовой моделью». Эти системы работают с ведома пользователя и, как правило, требуют их сотрудничества. Такой способ в ближайшем времени планирует ввести Сбербанк Российской Федерации.

Безопасность методов распознания оценивается с помощью таких терминов, как False Acceptance Rate (далее – FAR) и False Rejection Rate (далее – FRR). FAR – это коэффициентный порог, определяющий риск ошибочной идентификации одного человека за другого, и считается путем отношения числа ложных подтверждений, деленное на число попыток идентификации. FRR – это вероятность того, что биометрическая система безопасности ошибочно отклонит попытку доступа авторизованного пользователя, и определяется путем отношения числа ложных распознаваний, деленное на число попыток идентификации. Процент коэффициентов рассчитывается вручную по математическим формулам в зависимости от предназначения оборудования.

В сборнике практических рекомендаций организации объединенных наций предусмотрено, что правление рисками в системе предусматривает каталогизацию сбоев в системе – как в одной из ее частей (например, в устройстве считывания биометрических данных), так и в системе в целом (в конфигурации системы), и определение способности таких сбоев создать риск ненадлежащего функционирования системы. При этом определяются угрозы и риски, затем проводится анализ последствий осуществления или использования угрозы, и, наконец, в необходимых случаях принимаются меры по смягчению последствий [1].

Наименьший процент риска ненадлежащего функционирования биометрических систем составляют следующие виды биометрии:

1) дактилоскопия (FAR 0,1 – 0,001%, FRR 0,3 – 0,9%);
2) идентификация по геометрии лица (FAR 0,1 – 0,001%, FRR 2,5 – 9,0%);
3) идентификация по радужной оболочке глаза (FAR – 0,00001%, FRR – 0,13%).

На основе выше приведенного, можно сделать вывод, что наиболее надежным видом биометрической идентификации является распознание по радужной оболочке глаза. Однако, некоторые методы в настоящее время являются не комфортными для идентифицируемого. Например, в связи с сегодняшней эпидемиологической обстановкой, многие граждане могут обеспокоится на счет гигиеничности прикосновения к сканеру, что в дальнейшем спровоцирует резкий рост заболевших.

В.П. Захаров писал, что правоохранительные органы в настоящее время осуществляют распознание с помощью автоматизированных дактилоскопических идентификационных систем. Перспективным является использование биометрических технологий для контроля доступа к компьютерам, компьютерным сетям и в помещения. Для идентификации личности на расстоянии можно использовать только метод распознавания по геометрии лица. Поэтому в системах интеллектуального видеонаблюдения правоохранительных органов, использование которых имеет стойкую тенденцию к росту, возможно использование именно этого метода. Учитывая позитивные и негативные стороны метода распознавания личности по радужной оболочке глаз, его можно считать перспективным для использования в системах защиты информации правоохранительных органов, наравне с дактилоскопической идентификацией [2, с. 47].

Однако, все ранее приведенные методы биометрической идентификации имеют как общие, так и различные друг от друга недостатки. К общему недостатку относится то, что все эти базы данных, где содержится биометрическая информация, подвержены взлому. Реализацию рассматриваемого пробела можно рассмотреть в ряде новостей от СМИ, когда очередная преступная организация фальсифицировала данные, к примеру документы, удостоверяющие личность, и с смогла проникнуть в государство путем обмана.

Что касается практики, где биометрическая идентификация показала себя то, можно рассмотреть на примере Великобритании. Рассматриваемые технология была применена в Уэльсе в конце мая 2017 г. В качестве вида идентификации использовался метод распознавания по геометрии лица. Как отмечает полиция камеры распознали подозреваемого и сравнили его изображение с фотографиями, которые уже находились в базе данных, в следствии гражданина быстро задержали [5].

Как указывалось выше, подобные биометрические технологии могут применяться в качестве обеспечения общественной и национальной безопасности, а также для предотвращения терактов, так как на протяжении достаточно продолжительного времени биометрическая идентификация показывает себя с наилучшей стороны.

Таким образом, можно сделать вывод, что биометрические технологии – это мощный и действенный инструмент для борьбы с терроризмом на международном уровне. Она не только позволяет выявлять и пресекать деятельность террористических организаций, но и защищать население в целом от различных нападений. Основу идентификации составляет сбор, хранение, использование, передача персональных биометрических данных. Как отмечалось ранее, информация должна быть полностью защищена законодательством, а ее обработка или иные манипуляции должны осуществляться без нарушения основных прав человека, в том числе право на неприкосновенность частной жизни. В связи с ранее перечисленным фактами и доводами, можно сделать вывод, что наиболее распространенным методом среди видов биометрической идентификации является дактилоскопия.

ЛИТЕРАТУРА

1. Сборник практических рекомендаций Организации Объединенных Наций по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом [Электронный ресурс]. – Режим доступа: www.unodc.org/pdf/terrorism/Compendium-Biometrics/_.pdf – Дата доступа: 28.04.2020.
2. Захаров, В.П. Биометрические технологии в антитеррористической деятельности правоохранительных органов: перспективы и проблемы использования / В.П. Захаров, О.И. Зачек, М.С. Бекмурзин – Вестник Московского университета МВД России, 2014. – № 10. – 47 с.
3. Резолюция 1624 (2005), принятая Советом Безопасности на его 5261-м заседании 14 сентября 2005 года [Электронный ресурс]. – Режим доступа: undocs.org/ru/S/RES/1624(2005) – Дата доступа: 20.09.2020.
4. Резолюция 2396 (2017), принятая Советом Безопасности на его 8148-м заседании 21 декабря 2017 года [Электронный ресурс]. – Режим доступа: undocs.org/ru/S/RES/2396(2017) – Дата доступа: 20.09.2020.
5. Британская полиция впервые использовала новую технологию распознавания лиц [Электронный ресурс] – Режим доступа: news.rambler.ru/world/37099817-britanskaya-politsiya-vpervye-ispolzovala-novuyu-tehnologiyu-raspoznavaniya-lits/. – Дата доступа: 20.09.2020.