СБОРНИК ПРАКТИЧЕСКИХ РЕКОМЕНДАЦИЙ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ

по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом

Подготовлен совместно с Институтом биометрии

Сборник практических рекомендаций Организации Объединенных Наций
по ответственному использованию биометрических данных
и обмену ими в рамках борьбы с терроризмом
Окончательный проект

Содержание

Перевод этого сборника на русский язык был осуществлен благодаря щедрому вкладу Соединенных Штатов Америки.

2. Резюме

В настоящем Сборнике практических рекомендаций содержится общий обзор биометрических технологий и систем их использования в контексте борьбы с терроризмом. Сборник предназначен прежде всего для государств-членов, возможно не имеющих или почти не имеющих опыта работы с биометрическими приложениями, а также возможно испытывающих трудности с получением технической помощи и наращиванием потенциала в процессе внедрения этих технологий.

В конце каждого раздела приводится обширный список дополнительной литературы для изучения, а также краткая информация о рекомендуемых практических методах. Во всех разделах сборника содержатся конкретные примеры применения передовой практики и новых технологий.

В первом разделе дается общее представление об основных компонентах биометрической технологии и управления идентификационными данными, в том числе о широком использовании биометрии в криминалистике и расследованиях, проводимых правоохранительными органами, а также о связанных с этим дополнительных трудностях.

В следующем разделе речь идет о требованиях, касающихся управления, и нормативных требованиях к биометрической технологии с точки зрения международного права, стандартов в области прав человека, оценки соблюдения этических норм, требований к защите данных и права на неприкосновенность частной жизни. Далее следует общий обзор потенциальных факторов уязвимости биометрических систем и некоторых мер контроля, которые можно применять для снижения этих рисков. Затем рассматриваются международные технические и научные стандарты деятельности, касающиеся сертификации и аккредитации биометрических приложений, а также систем управления качеством, используемых при проведении соответствующих экспертно-криминалистических процедур. В последней части этого раздела рассматриваются требования, предъявляемые к закупке биометрических систем или сетей, предназначенных для борьбы с терроризмом, их техническому обслуживанию и обеспечению ресурсами, и, в частности, ключевые операционные и финансовые решения, которые необходимо принимать в процессе оценки возможного внедрения новой системы или модернизации существующей.

В последнем разделе содержится общий обзор предназначенных для борьбы с терроризмом биометрических систем и баз данных, применяемых в настоящее время правоохранительными органами, органами пограничного контроля и военными структурами. В нем также рассматриваются преимущества обмена биометрическими данными на двусторонней и многосторонней основе, в региональных и глобальных масштабах, а также способы использования биометрических данных — в сочетании с другими оперативными данными — не только в качестве традиционного следственного инструмента, но и для предотвращения террористических актов. Далее меры, принимаемые властями в случае совпадения биометрических данных, рассматриваются в контексте международных стандартов прав человека и необходимости принятия ответных мер на принципах полной информированности, законности и соразмерности. В заключительной части этого раздела речь идет о включении биометрических данных в стратегии борьбы с терроризмом, применяемые государствами — членами и регионами, а также о важной роли пограничных и правоохранительных органов в оказании активной поддержки таких стратегий.

Сборник представляет собой постоянно обновляемый документ с хронологической регистрацией изменений, с тем чтобы обеспечивать:

- его актуальность и отражение в нем быстрых темпов технических инноваций и научного прогресса в сфере биометрии; и
- гибкое и эффективное реагирование на возникновение и постоянное изменение характера угроз международного терроризма.

3. Предисловие

Резолюция 2322 (2016) Совета Безопасности об укреплении международного сотрудничества правоохранительных и судебных органов в вопросах борьбы с терроризмом прямо призывает государства-члены обмениваться информацией, в том числе биометрическими и биографическими данными, об иностранных боевиках-террористах (ИБТ) и других одиночных террористах и террористических организациях. В своей резолюции 2396 (2017) Совет постановил, что государства-члены должны в соответствии с внутренним законодательством и нормами международного права в области прав человека разрабатывать и внедрять системы сбора биометрических данных, которые могут включать отпечатки пальцев, фотографии, данные распознавания лиц и другие соответствующие идентификационные биометрические данные, для ответственного и надлежащего выявления террористов, включая ИБТ. Резолюция также призывает государства делиться этими данными, сообразно обстоятельствам, с другими государствами, а также с Международной организацией уголовной полиции (Интерполом) и другими соответствующими международными органами.

Эффективный обмен биометрическими данными крайне важен для расследования транснациональных преступлений и идентификации террористов. При проведении расследований по делам, связанным с терроризмом, биометрические технологии и другие методы судебной экспертизы могут быть крайне полезны для следователей и обвинителей, помогая им, помимо прочего, установить связь какого-либо лица с конкретным деянием, событием, местом, материалом или с другим лицом. Именно поэтому столь важно наращивать потенциал государств-членов в этой сфере.

Настоящий Сборник примеров надлежащей практики и рекомендаций разработан Рабочей группой по вопросам управления границами и правоохранительной деятельности в контексте борьбы с терроризмом в рамках Целевой группы по осуществлению контртеррористических мероприятий (ЦГОКМ) при финансовом содействии со стороны Контртеррористического центра Организации Объединенных Наций (КТЦООН), действующего в структуре Контртеррористического управления Организации Объединенных Наций (КТУ ООН). В Сборнике рассматриваются такие ключевые вопросы, как управление, регулирование, защита данных, политика соблюдения конфиденциальности, права человека, а также управление риском и оценки уязвимости.

Правительства должны внимательно отнестись к вопросу о последствиях использования этих технологий для прав человека, чтобы защитить людей, идентифицированных такими системами, от злоупотреблений и гарантировать проведение мероприятий на этапе планирования и на последующих этапах в соответствии с предусмотренными международным правом обязательствами, закрепленными в международных и региональных конвенциях о правах человека. Биометрия, как и все другие меры безопасности, имеет свои уязвимости. Поэтому огромное значение имеет то, каким образом эти уязвимости обнаруживаются, трактуются и сводятся к минимуму. Тщательная разработка, правильное введение биометрических данных и порядок установления параметров совпадения являются условиями, определяющими успешность применения этой технологии. Для обнаружения спуфинга[1], противодействия ему и снижения риска таких атак может быть использован целый ряд технологий — как программных, так и аппаратных.

Данный Сборник был разработан в партнерстве с Институтом биометрии — некоммерческой организацией, выступающей за ответственное и этичное использование биометрической информации и представляющей собой независимый и беспристрастный форум пользователей биометрической информации и других заинтересованных сторон. Благодаря тесному сотрудничеству Института биометрии с Исполнительным директоратом Контртеррористического комитета (ИДКТК) для руководства разработкой Сборника был сформирован международный консорциум экспертов, в состав которого вошли правительственные эксперты и специалисты в области биометрии, обладающие опытом работы в сфере борьбы с терроризмом, охраны правопорядка, пограничного контроля, биометрических технологий, обеспечения конфиденциальности и защиты данных.

Подготовка Сборника велась в рамках долгосрочного проекта по укреплению потенциала государств и соответствующих международных и региональных структур в области сбора, записи биометрических

[1] Спуфинг (известный также как представление ложного идентификатора) — это представление фальсифицированных биометрических данных (например, латексной маски, фотографии, поддельного отпечатка пальца или поддельной записи голоса) легального зарегистрированного пользователя для получения несанкционированного доступа к системе биометрического распознавания.

данных террористов, в том числе ИБТ, и обмена этими данными в соответствии с упомянутыми выше резолюциями Совета Безопасности. Осуществлением этого проекта в области биометрии занимается ИДКТК совместно со структурами, входящими в ЦГОКМ, к числу которых относятся Интерпол, Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН), Международная организация гражданской авиации (ИКАО) и Управление Верховного комиссара Организации Объединенных Наций по делам беженцев (УВКБ ООН). Цель проекта заключается в повышении уровня информированности о региональных и международных инициативах, направленных на содействие использованию биометрических данных, в укреплении координации и сотрудничества между соответствующими органами, в расширении масштабов использования биометрических данных и обмена ими на глобальном уровне, в том числе путем систематического внесения биометрической информации по профилям террористов в базы данных и уведомления Интерпола, а также в повышении эффективности помощи, предоставляемой государствам-членам в этой сфере.

Владимир Воронков
заместитель Генерального секретаря,
глава Контртеррористического управления
Организации Объединенных Наций,
исполнительный директор
Контртеррористического центра
Организации Объединенных Наций

Мишель Конинкс
помощник Генерального секретаря,
директор-исполнитель
Исполнительного директората
Контртеррористического комитета

Институт биометрии

Институт биометрии — некоммерческая организация, выступающая за ответственное и этичное применение биометрической информации, приветствует возможность оказать поддержку этому проекту. Институт биометрии является независимым и беспристрастным международным форумом для пользователей биометрической информации и других заинтересованных сторон. Его задача заключается в том, чтобы просвещать и информировать его членские организации, ключевые заинтересованные стороны и широкую общественность по вопросам биометрии, содействовать разработке стандартов, политики и передовой практики и повышать уровень осведомленности о них, а также обеспечивать безопасность и надежность биометрических систем и программ.

Созданный в 2001 году, Институт имеет представительства в Лондоне и Сиднее. Его членами являются свыше 230 организаций из 30 различных стран, представляющие широкий спектр пользователей, в том числе государственные ведомства, пограничные службы, правоохранительные органы, банки и авиакомпании, а также исследовательские организации, компании-поставщики и структуры, специализирующиеся на вопросах неприкосновенности частной жизни. Институт не занимается продвижением биометрических технологий, уделяя основное внимание ответственному использованию систем биометрии, их безопасности и целостности, а также — и это главное — вопросам неприкосновенности частной жизни и защиты данных. Институт признает, что системам биометрии присущи характерные факторы уязвимости, которые необходимо выявлять и смягчать их воздействие.

Биометрия, неприкосновенность частной жизни и права человека

Применение биометрии приобретает все более повсеместный характер, и одновременно с этим общественность все в большей степени приемлет эту технологию, пользуясь биометрическими технологиями в мобильных телефонах, но не всегда осознавая при этом возможные последствия. Это указывает на необходимость повышения осведомленности о преимуществах и рисках применения биометрических технологий. Биометрия удобна и может обеспечить более высокий уровень безопасности. При этом, однако, требует решения ряд проблем, таких как защита права на неприкосновенность частной жизни, защита данных и борьба со спуфингом. Персональные данные, в том числе биометрические, следует собирать и хранить лишь в тех случаях, когда это одновременно и необходимо, и целесообразно.

Биометрия способна играть все более важную роль в глобальной борьбе с терроризмом, а именно в противодействии мошенничеству, хищению личных данных и других уголовных преступлений,

совершаемых террористами в целях поддержки своей деятельности. Вместе с тем, чтобы в полной мере реализовать потенциал биометрических технологий, правительствам необходимо решать вопросы, связанные с защитой лиц, идентифицируемых такими системами, добиваясь, чтобы сбор, хранение и использование биометрических данных велись в соответствии с международными стандартами в области прав человека и международными законами о неприкосновенности частной жизни, в том числе Международным пактом о гражданских и политических правах (МПГПП) и Всеобщей декларацией прав человека Организации Объединенных Наций (ВДПЧ).

Необходимо защитить лиц, у которых были украдены их биометрические/идентификационные данные или которые просто стали жертвой ошибки в системе. Восстановление идентификационных данных человека — более сложная задача, чем просто восстановление пароля. Биометрические данные человека остаются у него на протяжении всей жизни, и здесь необходимы самые тщательные меры предосторожности. В настоящем Сборнике приводится обзор проблем и возможных решений такой сложной задачи, как сочетание эффективных стратегий борьбы с терроризмом с правом на неприкосновенность частной жизни и другими правами человека.

Факторы уязвимости биометрических систем и атаки на эти системы

У биометрии, как и у любых других мер безопасности, есть уязвимые места. Основной вопрос заключается в том, как свести такие уязвимости к минимуму. Тщательная разработка, правильное введение биометрических данных и порядок установления параметров совпадения являются условиями, определяющими успешность применения этой технологии. Слишком жесткие параметры могут стать причиной «ложноотрицательного результата», когда разрешенному пользователю будет отказано в доступе. Недостаточно жесткие параметры могут повлечь за собой «ложноположительный результат», когда доступ будет предоставлен пользователю-злоумышленнику.

Институт биометрии принял разумные меры по обеспечению достоверности материалов, представленных в настоящем Сборнике. С учетом того что в процессе внедрения биометрических технологий и после его завершения могут изменяться содержание Сборника и вводимые переменные, Институт не несет ответственности за результаты использования Сборника или соблюдение предложенных в нем рекомендаций. Сборник был подготовлен исключительно в информационных целях и не может рассматриваться как справочник по правовым вопросам или вопросам соответствия нормам законодательства.

Эндрю Райс
председатель и директор
Института биометрии

Изабель Мёллер
исполнительный директор
Института биометрии

4. Введение в биометрические системы и средства идентификации личности

В разделе 4 дается общее представление об основных компонентах биометрических технологий и управления идентификационными данными, в том числе о широком использовании биометрии в криминалистике и расследованиях, проводимых правоохранительными органами, а также связанных с этим дополнительных трудностях.

Человек — это социальное животное, наделенное исключительной способностью узнавать и, соответственно, различать знакомых ему людей. Вместе с тем у человека сильно развито чувство собственного «я» и ощущение собственной уникальности. Наши социальные инстинкты побуждают нас считать себя уникальной личностью и признавать уникальность других индивидуумов. На биологическом уровне люди уникальны (во всех практических отношениях). Вместе с тем наш «механизм распознавания человека» не является биологически обусловленным, и на деле люди плохо различают тех, с кем они незнакомы. Применяемые людьми системы идентификации личности также не работают на основе биологии. В таких системах используются те или иные сочетания идентификационных и контекстуальных

признаков, которые выступают в качестве маркеров, представляющих описываемую биологическую особь, но не идентичных ей[2].

К числу идентификационных признаков относятся имя, дата и место рождения, гражданство, пол и биометрические[3] идентификаторы. Контекстуальные признаки — это оперативная информация, чаще всего касающаяся места и времени. Использование контекстуальных признаков повышает точность идентификации. Идентификационные признаки могут быть биографическими или биометрическими и при определенных обстоятельствах могут изменяться. Так, например, изменяться могут следующие биографические идентификационные признаки:

- имена — могут являться объектом транслитерации, т.е. одно и то же имя может иметь разные варианты написания;
- дата рождения — может быть зарегистрирована с опозданием, или же в официальных документах могут быть разночтения;
- место рождения — может быть записано по-разному;
- пол — может зависеть от личных предпочтений человека, измениться в результате хирургического вмешательства и т.д.;
- гражданство — может быть множественным и изменяться.

На протяжении жизни человека биометрические идентификационные признаки могут в процессе роста или старения или под влиянием болезни изменяться, т.е. может изменяться относительный размер, степень четкости и различимость конкретных отличительных черт. У некоторых людей биометрические признаки могут быть повреждены или отсутствовать вовсе. Так, например, отпечатки пальцев формируются на ранних стадиях развития плода и, при отсутствии повреждений, остаются неизменными на протяжении жизни; они могут также сохраняться на протяжении значительного периода времени и после смерти, особенно в теплой и сухой среде, которая высушивает кожу. Хотя рисунок завитков на отпечатке пальца не изменяется, сам палец изменяется в размерах в течение жизни человека, а качество отличительных признаков отпечатка пальца может ухудшаться под воздействием неблагоприятной внешней среды, из-за повреждений или в процессе старения. Аналогичные изменения могут претерпевать и другие биометрические признаки. Соответственно, алгоритмы, применяемые сегодня в биометрических приложениях, разработаны с учетом разумных поправок на такие изменения, с тем чтобы обеспечить возможность регистрировать и сохранять в системе данные как можно большего числа людей, независимо от их возраста или незначительного ухудшения качества их биометрических признаков.

Биометрические маркеры представляют собой идентификационные признаки и, обладая высокой степенью репрезентативности в отношении описываемого ими человека, составляют надежную основу для сопоставлений в цифровом формате. Однако, как и биографические идентификационные признаки, биометрические образцы, зафиксированные в формате изображения или преобразованные в шаблон или профиль, отличаются от описываемой ими биологической особи. Процесс фиксирования и записи идентификационных признаков, в том числе биометрических, всегда неполон и несовершенен, и поэтому в его ходе могут появляться ошибки. Вероятностное совпадение, свойственное биометрическим сопоставлениям, может быть подвержено статистической дисперсии. Наличие ошибок и статистической дисперсии в системах распознавания человека делает их потенциально уязвимыми для разного рода атак (см. раздел 5.3), и противодействовать этому можно путем внедрения надежных средств защиты и проведения их систематического обновления в рамках процедуры управления риском в системе[4]. Сведение к минимуму таких свойственных системам распознавания человека уязвимостей — один из основных вопросов, рассматриваемых в данном Сборнике.

---

[2] *Identity verification- The importance of context and continuity of identity*, p. 11-16 Keesing Journal of Documents & Identity, Annual Report Identity Management 2011-2012.

[3] В 1995 году Биометрический консорциум при правительстве США дал следующее определение биометрии: «…автоматизированная система распознавания отдельных лиц на основании их поведенческих и биологических характеристик».

[4] «Системы распознавания людей неизбежно носят вероятностный характер и поэтому неизбежно могут давать сбои. Вероятность ошибки можно уменьшить, но ее нельзя свести к нулю. Разработчикам и операторам систем необходимо предвидеть возможность ошибок и иметь на этот случай соответствующие планы, даже если эти ошибки, как ожидается, будут нечастыми». Page 1, *Biometric Recognition: Challenges and Opportunities, National Research Council, Washington (2010), доступно для скачивания на сайте* http://www.nap.edu/openbook.php?record_id=12720&page=1.

Биометрические системы призваны обеспечить распознавание человека с использованием его биологических и физиологических характеристик, таких, например, как отпечатки пальцев, рисунок вен на тыльной стороне ладони, радужная оболочка глаза, лицо, ДНК и т.д.[5] Каждая такая характеристика представляет собой биометрическую модальность. Выбор одной или нескольких наилучших биометрических модальностей зависит от условий, в которых осуществляется вариант их использования (см. раздел 5.5). В целом все биометрические модальности обладают общими особенностями[6], которые — в большей или меньшей степени — определяют их.

- Универсальность — они есть у каждого человека (за исключением тех, у кого биометрические признаки были повреждены или отсутствуют).
- Уникальность — они должны обеспечивать возможность проводить различие между лицами, зарегистрированными в системе. При этом для отдельных модальностей возможны варианты: например, у близнецов будет одинаковый профиль ДНК, но разные отпечатки пальцев.
- Постоянство — они должны оставаться стабильными и неизменными на протяжении длительного периода времени, чтобы обеспечить возможность применения алгоритма сопоставления при учете изменений, возникающих в течение жизни человека.
- Измеримость — они должны легко поддаваться сбору и оцифровке в рамках системы.
- Эффективное функционирование — они должны быть точными, быстрыми в обработке и надежными как на начальном, так и на последующих этапах технологического процесса.
- Приемлемость — они должны соответствовать социальным нормам и представлениям, и ими должна обладать значительная часть лиц, чьи данные предполагается внести в систему.
- Уязвимость к возможным действиям в обход — потенциально злоумышленники могут получить санкционированный доступ с помощью различных приспособлений и устройств-«обманок»; для противодействия этому необходимо принимать и постоянно совершенствовать жесткие контрмеры.

Поскольку многие биометрические системы предполагают сопоставление с контрольными данными, ключевым фактором выбора предпочтительной модальности является наличие ранее собранных данных, которые сведены или могут быть сведены в пригодную для использования и полезную базу справочных данных, позволяющую проводить и подтверждать идентификацию. В системах может использоваться только одна модальность (мономодальная система), например распознавание по лицу, или несколько модальностей в сочетании (мультимодальная система), например отпечатки пальцев, радужная оболочка глаза и лицо. В настоящее время быстро увеличивается количество приложений с применением биометрических систем, используемых в государственном и коммерческом секторах, в том числе:

- национальные реестры актов гражданского состояния, обеспечивающие доступ к государственным услугам на местном и национальном уровнях;
- водительские удостоверения;
- архивы уголовного судопроизводства;
- расследование преступлений;
- системы видеонаблюдения;
- обеспечение безопасности границ/системы выдачи паспортов;
- помощь беженцам;
- финансовые услуги;
- компьютерные системы;
- базы данных с защищенным доступом;

[5] **Примечание.** В настоящем Сборнике речь идет главным образом о тех физических биометрических признаках, которые связаны с идентичностью человека (лицо, отпечатки пальцев, ДНК и т.д.), а не с его поведением. К числу поведенческих биометрических модальностей относятся, например, походка, характеристика работы с клавиатурой и пользования компьютерной мышью, собственноручная подпись и т.п., определяющие особенности деятельности человека.

[6] Список составлен по материалам: Jain et al “Biometrics: Personal Identification in Networked Society”, Norwell, Mass.: Kluwer Academic Publisher (1999).

- доступ к месту проведения мероприятий;
- доступ к смартфонам;
- управление идентификацией пользователей в системе здравоохранения;
- учет присутствия на рабочих местах.

Модальности, используемые в этих приложениях, позволяют идентифицировать человека, даже если он предоставляет фальшивые данные или пытается выдать себя за другого. Эти неоценимые функциональные возможности могут быть эффективно использованы для отслеживания и выявления террористов и пресечения их деятельности в глобальном масштабе. В сфере биометрии сложилась плодотворная обстановка для активных и энергичных коммерческих исследований и разработок по актуальным направлениям, и на рынке постоянно появляются новые приложения и новые модальности.

Стандартная операционная модель базовой биометрической системы, используемой, например, для контроля доступа, включает перечисленные ниже этапы.

- *Сбор и введение данных* — получение биометрического образца человека (субъекта) с использованием устройства для сбора данных. Процедуру сбора данных можно проводить с использованием либо устройства, постоянно находящегося в определенном месте, либо мобильного устройства с возможностью дистанционной загрузки данных. Биометрические данные можно получать посредством контакта с устройством для сбора данных (например, отпечатки пальцев), в непосредственной близости к нему, как, например, в случае получения изображения лица, или дистанционно. Вместе с тем важнейшим критерием успешности любой такой системы является качество введенных биометрических данных. Плохое качество введенных данных существенно снизит и эффективность системы, поэтому крайне важно собирать биометрические данные неизменно высокого качества, что позволит обеспечивать оптимальную способность к распознаванию (см. раздел 5.3.4).
- *Извлечение данных* — конвертация полученного образца в биометрический шаблон. Например, отпечаток пальца в целях его сохранения, проведения поиска и сопоставления может быть преобразован в цифровой формат. Соответственно, процедура извлечения данных призвана преобразовать исходное изображение или первоначальный образец в пригодный для использования и эффективный набор данных в цифровом формате, который может быть с большой точностью разыскан и сопоставлен с контрольными образцами в базе данных и который занимает намного меньше места в системе, нежели исходное биометрическое изображение/образец.
- *Хранение данных* — сохранение введенных данных в системе или базе данных, иногда ограничивающееся одним шаблоном на человека по завершении стадии поиска/сравнения. Большинство устройств для сбора данных выгружают данные на сервер или в центральную базу данных для проведения поиска, тогда как некоторые мобильные устройства имеют собственную интегрированную базу данных и поэтому могут использоваться дистанционно, без подключения к какому-либо другому оборудованию.
- *Сопоставление данных* — получение доступа к базе данных и извлечение одного или нескольких введенных ранее шаблонов для сопоставления с представленным.
- *Определение соответствия данных* — использование компьютерных алгоритмов для определения того, соответствует ли исследуемый шаблон шаблону (шаблонам), выбранному(ым) из базы данных. Как правило, исследуемый шаблон не сохраняется, если он был признан соответствующим контрольному шаблону из базы данных.
- *Результат* — полученная в итоге оценка «соответствует» или «не соответствует» определяет дальнейшую работу системы в целом. Например, если задача биометрического компонента — подтвердить личность человека, внесенного в базу данных лиц, имеющих право на вход в охраняемое здание, то оценка «соответствует» по результатам сопоставления с контрольным шаблоном идентификации разрешит вход, а оценка «не соответствует» в праве на вход откажет.

Вместе с тем не все приложения используют подтвержденные идентификационные признаки, поскольку в биометрических системах применяются два принципиально разных процесса. Первый процесс, предусматривающий использование подтвержденной идентичности, представляет собой:

верификацию (известную также как сопоставление одного с одним, или 1:1). В этой модели подтвержденная идентичность применяется для того, чтобы выбрать из базы данных или электронного документа только один шаблон и сопоставить его с исследуемым шаблоном. В ходе этого процесса проводится сопоставление исследуемого шаблона с шаблоном из базы данных и либо подтверждается, что оба шаблона соответствуют одному и тому же лицу, либо это не подтверждается.

В процессе верификации задается вопрос «Являетесь ли вы тем же самым лицом, чья идентичность уже была удостоверена и введена в систему?».

Второй процесс — модель поиска — предусматривает:

идентификацию (известную также как сопоставление одного со многими, или 1:n). В этом случае поиск ведется без учета предполагаемой идентичности, и поэтому исследуемый шаблон сопоставляется со всеми шаблонами в базе данных на предмет возможного соответствия. Программа поиска и определения соответствия устанавливает степень сходства для потенциальных случаев соответствия и либо автоматически выбирает шаблон с высокой долей вероятности соответствия, либо представляет список шаблонов с предполагаемым соответствием оператору, который и сопоставляет их с исследуемым шаблоном.

В процессе идентификации задается вопрос «Внесены ли вы в справочную базу данных, и если да, то какому шаблону вы соответствуете?».

Значимость и особенности результатов, получаемых от систем как верификации, так и идентификации, зависят от того, какая именно операционная модель применяется в приложении. Например, в некоторых случаях положительная идентификация будет обычным результатом, а отрицательный результат — исключением (например, если речь идет о доступе сотрудников в охраняемую зону), тогда как в других моделях нормальным будет считаться отрицательный результат, а положительный будет исключением (например, когда всех пассажиров проверяют на предмет совпадения их данных с биометрическими данными лиц, связанных с террористической деятельностью и внесенных в список подозреваемых лиц). Эффективные биометрические системы объединяют раздельные задачи по верификации и идентификации в целях повышения надежности установления идентичности и достоверности сопоставлений со справочными базами данных.

Пользователям может казаться, что многие биометрические приложения автоматизированы полностью — от сбора данных до получения результата, однако часто в более сложных системах вмешательство человека оказывается необходимым на разных стадиях процесса для обеспечения бесперебойной работы этих систем, хотя для пользователя это может и не быть очевидно. На фоне продолжающегося стремительного наращивания вычислительных мощностей и появления новых технологий обработки данных потребность во вмешательстве человека быстро снижается, однако, хотя и можно ожидать, что автоматическое сопоставление биометрических образцов станет нормой, в более сложных случаях установление связи между совпавшими образцами и другими идентификационными и контекстуальными признаками будет, скорее всего, по-прежнему осуществляться человеком.

Пример из практики 1. Биометрия на границах

При проведении процедуры выдачи путешествующим разрешения на пересечение границы, осуществляемой методом верификации 1:1, и процедуры оценки рисков в связи с путешествующими, проводимой путем сопоставления 1:n со списками подозреваемых лиц и базами оперативных данных, происходит взаимный обмен информацией (см. рисунок 1). Идентификационные признаки, фигурирующие в списках подозреваемых лиц и базах оперативных данных, как правило, неполны. Это происходит потому, что лица, подлежащие включению в список подозреваемых лиц, идентифицируются на основании разных критериев и в разных обстоятельствах. Не всегда в каждом списке подозреваемых лиц или списке, составленном оперативно-разыскной службой, указываются все биографические или биометрические данные. Контекстуальные признаки не являются исчерпывающими. В отношении всех элементов, внесенных в списки подозреваемых лиц и базы оперативных данных, существует возможность ошибки.

Сопоставление	Источник справочных данных	Основан для сопоставления биографических данных	Основан для сопоставления биометрических данных	Связь с контекстуальными признаками
Вертификация 1:1	Проездные документы	• Имя • Дата рождения • Пол • Гражданство	• Черты лица • Отпечатки пальцев • Радужная оболочка глаза	• Место и время • Гражданство • Проверка проездных документов
Идентификация 1:n	– Контрольные списки – Оперативные данные	• Имя • Дата рождения • Пол • Гражданство	• Черты лица • Отпечатки пальцев • Радужная оболочка глаза • Голос • ДНК	• Место и время • База данных Интерпола о похищенных и утерянных проездных документах • Предшествующие события • Сопутствующие признаки (мобильный телефон, переписка по электронной почте и т.д.)

Рисунок 1 подготовлен на основе *ICAO TRIP Guide on Border Control Management, Montreal (2018)*
(с разрешения ИКАО)

Верифицированные идентификационные данные позволяют с большей долей надежности увязывать между собой биографические, биометрические и контекстуальные данные, что, соответственно, повышает эффективность поиска по контрольным спискам и базам оперативных данных. Сопоставление биометрических данных играет при этом очень важную роль, однако использование сопоставления только лишь таких данных не может определять результаты сравнения идентификационных признаков[7].

4.1. Эффективность системы

Эффективность любой биометрической системы в значительной мере определяется 1) сферой и масштабами ее предполагаемого применения; 2) выбором наиболее подходящей модальности или модальностей для поддержки такого применения; 3) надежностью, последовательностью и своевременностью обработки данных в сочетании с минимальным техническим обслуживанием. К числу основных показателей эффективности биометрической системы относятся точность, частота ошибок[8], пропускная способность, а также объем и скорость обработки исключений. В общем и целом, точность — это показатель способности системы обеспечить правильное сопоставление биометрических идентификационных признаков одного и того же лица, не допуская при этом ошибочного сопоставления биометрических идентификационных признаков разных лиц. Для определения степени точности биометрической системы используются следующие показатели, выражаемые в процентах либо в долях и обычно рассчитываемые на основании эксплуатационных испытаний или лабораторных экспериментов.

Вероятность правильного допуска (TAR) — показатель способности системы правильно сопоставлять признаки биометрической идентичности одного и того же лица.

Вероятность ложного допуска (FAR) — ложный допуск имеет место в тех случаях, когда система ошибочно находит совпадение исследуемого биометрического шаблона одного лица с биометрическим шаблоном другого лица, внесенного в базу данных. FAR представляет собой отношение числа случаев ложного допуска к общему числу запросов на биометрическую идентификацию, на которые должен был

[7] Подробнее см. ICAO TRIP Guide on Border Control Management, Montreal (2018).

[8] Для расчета частоты ошибок требуется абстрагирование и допущение закрытого множества, что позволяет провести затем сопоставление данных в базе по принципу «всех со всеми» и на этой основе рассчитать частоту ошибок. Такие расчеты нередко проводятся путем моделирования с применением стандартизированных баз данных, которые могут соответствовать, а могут и не соответствовать реальным данным. Абстракция частоты ошибок может быть полезна при разработке системы и прогнозировании эффективности верификации 1:1. В реальности, с учетом численности мирового населения, превышающей 7 млрд человек, попадание в базу заменяющих данных возможно, а в случае контрольных списков и баз оперативных данных — вполне предсказуемо. Показатели частоты ошибок следует использовать с осторожностью и только в отношении верификации. В реальности эффективность биометрических систем в части сопоставления признаков может существенно отличаться от прогнозируемой на основании смоделированных расчетов этого показателя.

быть дан отрицательный ответ, т.е. отношение числа несовпадений, *которые система определила и представила как совпадения*, к общему числу истинных несовпадений.

Вероятность правильного недопуска (TRR) — показатель количества случаев, когда было правильно установлено *несоответствие* биометрических идентификационных признаков одного лица биометрическим идентификационным признакам других лиц, внесенных в базу данных, т.е. частота случаев правильно определенных несовпадений.

Вероятность ложного недопуска (FRR) — ложный недопуск имеет место в тех случаях, когда исследуемый биометрический шаблон не определяется как соответствующий правильному шаблону из базы данных, хотя оба этих шаблона относятся к одному и тому же лицу. FRR представляет собой отношение числа случаев ложного недопуска к общему числу запросов, которые должны были быть удовлетворены, т.е. отношение числа совпадений, *которые система определила и представила как несовпадения*, к общему числу истинных совпадений.

Соответственно, при разработке системы необходимо повышать показатели TAR и TRR, стремясь свести при этом к минимуму показатели FAR и FRR. Проще говоря, при TAR в 70% FAR будет составлять 30%, тогда как при TAR в 97% FAR будет составлять всего 3%. Следует отметить, что точность в 100% не обеспечивает ни одна биометрическая система.

Вместе с тем между значениями FAR и FRR также существует тесная взаимосвязь, и предпочтительное соотношение между этими двумя показателями частоты ошибок в значительной мере определяется производственными целями использования конкретной биометрической системы. Например, если доступ сотрудника в помещения компании увязан с биометрическим приложением, тогда высокий показатель FRR будет регулярно затруднять сотрудникам возможности входа, тогда как слишком высокий показатель FAR будет постоянно открывать доступ лицам, не имеющим на это права. Соответственно, для такого приложения необходимо определить регулируемое пороговое значение, которое уравновешивало бы FRR и FAR и предоставляло сотрудникам беспрепятственный доступ, при этом не допуская в *большинстве* случаев несанкционированный вход. В случае когда требуется обеспечить более высокий уровень безопасности, необходимо изменить пороговое значение, чтобы предупредить несанкционированный доступ, и для этого понизить, насколько это возможно, FAR, даже повысив при этом FRR и затруднив тем самым проход тем сотрудникам, которые имеют на это право. Таким образом, такое пороговое значение часто является определяемым практическими соображениями компромиссом между FRR и FAR, позволяющим оптимизировать эффективность системы в рамках конкретного применения и определяющим соотношение между необходимостью обеспечить безопасность, с одной стороны, и удобством для сотрудников, скоростью обработки и общими затратами на эксплуатацию системы, с другой. Под уровнем равной вероятности ошибок (EER)[9] понимается такое установленное для определенных модальностей пороговое значение, при котором FAR и FRR равны, например когда доля ошибки приема совпадает с долей ошибки отклонения.

На точность влияют и другие факторы, например вероятность отказа сбора данных (FTA), представляющая собой в общем и целом ту долю всех зафиксированных транзакций, для которых системе не удалось завершить процесс регистрации из-за сбоев на стадиях представления данных (например, не было получено изображение), отбора характерных признаков или контроля качества. Сюда относятся, помимо сбоев в системе, еще и случаи, когда биометрические данные человека повреждены, испорчены или отсутствуют. FTA является важным показателем реальных операционных возможностей системы. Высокий показатель FTA требует использования альтернативных методов сбора биометрических данных у лиц, не имеющих возможности по той или иной причине зарегистрироваться в системе. В таких случаях могут использоваться аналогичные, но при этом альтернативные биометрические признаки, например отпечаток большого пальца не правой, а левой руки, или же может быть дополнительно предусмотрена возможность распознавания другого биометрического признака, и для этого потребуется разработка мультимодальной системы. Если использование этих вариантов не представляется возможным, может быть применена методика без использования биометрии, известная как обработка исключений. Например, проверку личности человека, чьи биометрические данные не могут быть введены в систему, может проводить оператор, или же могут применяться менее защищенные методы, такие как ПИН-код или личная подпись. Во всех подобных случаях общая эффективность системы может быть значительно снижена. Поэтому мультимодальные биометрические приложения часто оказываются более предпочтительными, так как они обеспечивают более высокие показатели регистрации и снижают FTA.

[9] Известен также как уровень пересечения вероятности ошибок.

Пропускная способность определяет количество лиц, которые могут получить доступ в систему в течение определенного промежутка времени, т.е. соотношение производительности и скорости. Например, аэропорт, в котором допуск пассажиров проводится с использованием биометрических электронных паспортов, должен будет рассчитать нынешний и будущий пассажиропоток, чтобы установить достаточное количество стоек биометрической регистрации, позволяющее эффективно регулировать потоки пассажиров в наиболее загруженное время. Это даст возможность обеспечить работу биометрических систем с заранее установленными показателями вероятности ошибок, как того требуют соображения безопасности, и при этом мгновенно проводить одновременно множество операций по верификации — к удовлетворению клиентов и в интересах эффективного ведения бизнеса.

4.2. Роль биометрии в криминалистике

Криминалистика в целом занимается вопросами обмена вещественными материалами или информацией на электронных цифровых носителях между людьми, объектами и местами. Эти материалы могут быть видимыми (например, брызги крови на стене), невидимыми (например, микроскопические следы пороховых газов или взрывчатого вещества) или же иметь форму электронного изображения (например, снимки лиц, сделанные камерами наружного наблюдения). Обмен такими материалами или данными может происходить до совершения преступного деяния, в процессе его совершения или после него. Некоторые подобные материалы содержат также *биометрическую* информацию, например потожировые следы пальцев на стеклянной посуде, голос, записанный в ходе телефонного разговора, или профиль ДНК, выделенный из слюны, оставленной на ободке чашки. Подобная «криминалистическая биометрическая информация»[10] представляет собой ключевой компонент криминалистики и важнейший элемент расследований, проводимых правоохранительными органами, поскольку она предоставляет возможности для идентификации людей. Эта информация имеет огромное значение и для эффективного проведения успешных контртеррористических операций, поскольку позволяет:

- подтвердить или опровергнуть причастность лица к правонарушению путем предоставления — как самостоятельно, так и в составе других доказательств — данных, либо подтверждающих вину, либо освобождающих от обвинения (см. пример из практики 2 в конце раздела 4.2);
- обеспечить проведение объективного и убедительного судебного процесса на принципах верховенства закона, тем самым снизив зависимость от признаний, полученных в ходе уголовного следствия, особенно если для их получения применялись пытки или другие меры принуждения;
- дать картину событий, происходивших на месте преступления и в связи с ним;
- найти связь данного лица с деянием, событием, местом или другим лицом до инцидента, в его ходе или после него;
- найти связь одного события с другим или с несколькими другими;
- выявить данные, находящиеся в различных электронных или цифровых системах, и найти связь между ними.

Для реализации этих возможностей необходима координация данных, получаемых от других соответствующих направлений судебной науки и других областей специальной технической и научной экспертизы[11]. Криминалистическое исследование всех материалов на месте преступления и в лаборатории должно вестись в соответствии с международными стандартами и соответствующими системами обеспечения качества (см. раздел 5.4.2). К числу основных направлений криминалистики относятся:

- биологическая экспертиза — исследование дезоксирибонуклеиновой кислоты (ДНК), биологических жидкостей, волос, тканей и т.д.;
- исследование отпечатков — отпечатков пальцев и ладоней, следов, оставленных инструментами, отпечатков обуви, следов шин и т.д.;
- исследование огнестрельного оружия и баллистика;

[10] Forensic Biometrics: from two communities to one discipline. Proceedings of the International Conference of the Biometrics Special Interest Group 2012 Sept 6-7; Darmstadt, Germany.

[11] Подробное описание многих таких методик приводится в двух публикациях Управления Организации Объединенных Наций по наркотикам и преступности: ‘Police: Forensic services and infrastructure’ и ‘Staff skill requirements and equipment recommendations for forensic science laboratories.’ (www.unodc.org)

- трасологический анализ — исследование краски, стекла, волокон, взрывчатых веществ и т.д.;
- цифровые и электронные доказательства — получение доступа к устройствам, загрузка данных, анализ, определение величины ущерба и т.д.;
- наркотики — идентификация и определение количества;
- анализ документов;
- анализ взрывчатых веществ.

Используемые в криминалистике биометрические материалы применяются при расследовании дел для проведения сопоставлений (например, сопоставления отпечатков пальцев, полученных на месте преступления, с отпечатками пальцев подозреваемого), а также представляют собой одну из трех основных типов баз данных, с которыми работают криминалисты[12].

1. *Справочные базы данных по материалам судебных дел* — например, коллекции натуральных и искусственных волокон, как правило предоставляемых производителями и торговцами и используемых для идентификации волокон, изъятых с мест преступления, их классификации и сопоставления.
2. *Поисковые базы данных небиометрических объектов* — например, огнестрельного оружия и боеприпасов, отпечатков обуви и т.п.
3. *Поисковые базы данных биометрических материалов* — коллекция биологических материалов и образцов, относящихся к человеку, например ДНК и отпечатков пальцев.

При работе с биометрическими образцами в рамках криминалистической экспертизы и следствия необходимо соблюдать базовые принципы работы с криминалистическими данными. В противном случае результаты, полученные при использовании системы поиска по биометрическим данным, окажутся бесполезными для любого последующего судебного разбирательства. Именно поэтому при изъятии любого образца/предмета с места преступления следует последовательно вести следующие записи и соблюдать следующие процедуры:

- *происхождение* — письменное фиксирование и фотографирование места нахождения образца/предмета;
- *сохранение* — образец/предмет, направляемый на криминалистическую экспертизу, должен быть изъят и упакован таким образом, чтобы не допустить его загрязнения, уничтожения, изменения, потери или разрушения; упаковка должна также защищать образец от повреждений при перевозке и не допускать, чтобы он получил загрязнение от других предметов или окружающего пространства; или сам стал источником их загрязнения; образец следует хранить при соответствующей температуре, чтобы обеспечить его сохранность и доставку в тестовом состоянии, оптимальном для проведения лабораторного анализа;
- *целостность* — упаковка должна быть прочной, ненарушенной и опломбированной, чтобы не допустить несанкционированного доступа или проникновения; нельзя допустить возможности внесения или удаления каких-либо материалов (в том числе в твердом, жидком или газообразном состоянии) сквозь упаковку;
- *непрерывность (система охраны вещественных доказательств при их передаче)* — следует вести учет всех лиц, имевших доступ к упакованному образцу/предмету, начиная с места преступления.

Пример из практики 2. Проект «Невиновность»

Проект «Невиновность» (The Innocence Project) был создан в 1992 году Полом Нойфелдом и Барри Шреком из Школы правоведения им. Бенджамина Н. Кардозо, Нью-Йорк, США. Цель проекта состоит в использовании профилей ДНК для оправдания необоснованно осужденных лиц и реформирования системы уголовного правосудия США для недопущения подобной несправедливости в будущем.

[12] Базы оперативных криминалистических данных часто находятся под управлением и в ведении криминалистов, работающих в лабораториях судебной экспертизы, однако базы некоторых биометрических данных, например отпечатков пальцев, ДНК, записей голосов и фотографий лиц, могут находиться в ведении других сотрудников правоохранительных органов.

Концепция проекта исходит из того, что если анализ ДНК может доказать виновность человека в совершении преступления, то он может также доказать невиновность людей, осужденных необоснованно. На настоящий момент анализы ДНК позволили оправдать 356 человек и выявить 153 возможных преступника.

4.2.1. Криминалистические базы биометрических данных: категории данных

Криминалистические лаборатории и правоохранительные органы постоянно пользуются криминалистическими базами биометрических данных, известными также как базы оперативных данных судебной экспертизы. Во многих странах эти базы данных уже свыше 100 лет играют существенную роль в проведении уголовных расследований, в частности по делам о терроризме. К числу наиболее широко используемых модальностей относятся отпечатки пальцев, ДНК, черты лица и записи голосов. В каждой базе данных содержатся наборы данных двух различных типов.

Эталонные данные — собираются в контролируемых условиях у арестованных за совершение правонарушения или подозреваемых в его совершении. К их числу относятся, например, отпечатки всех 10 пальцев рук, снятые электронным сканером или традиционным методом с использованием чернил и бумаги; ротовые мазки, взятые с внутренней стороны щеки арестованного, образцы волос или крови, которые затем обрабатываются для получения полного ДНК-профиля[13]; цифровые фотографии лица и т.п. Эталонные данные могут собираться также у сотрудников полиции и лиц, правомерно присутствовавших на месте преступления до, во время или после его совершения. Эти данные необходимы для идентификации оставленных такими лицами криминалистических материалов и их исключения из материалов следствия.

Данные с места преступления — к ним относятся образцы и предметы, собранные на месте преступления[14]. Качество биометрических данных с места преступления может быть очень разным. Полученные криминалистические материалы могут по разным причинам оказаться поврежденными, загрязненными, недостаточно полными или четкими. В связи с этим процедура поиска и сопоставления дает гораздо более широкий спектр результатов, чем обычные ответы «соответствует» — «не соответствует», которые дают различные биометрические системы, не относящиеся к сфере криминалистики, например приложения контроля доступа (см. раздел 4.5).

Некоторые страны используют также масштабные биометрические системы для регистрации своих граждан, такие, например, как системы оформления удостоверений личности. Это обеспечивает официальное подтверждение личности каждого гражданина, что дает ему доступ к государственным услугам и другим видам социального и коммерческого обслуживания, таким, например, как социальное обеспечение, обеспечение жильем, страхование, банковское обслуживание и т.д.

Системы регистрации актов гражданского состояния — в этих системах обычно используются такие модальности, как отпечатки пальцев, изображения лица, радужная оболочка глаза, или комбинации нескольких модальностей. В таких базах данных, предназначенных прежде всего для поиска справочной информации, могут храниться, в зависимости от численности населения страны, миллионы, десятки или сотни миллионов биометрических образцов (справочных данных). Поэтому, если нормативно-правовая система страны позволяет правоохранительным органам вести поиск по этим базам данных в целях расследования преступления, круг поиска обычно ограничивается только справочными данными. Это даст возможность определить по отпечаткам пальцев или изображению лица, был ли человек зарегистрирован в системе, однако попытка сличить отпечатки пальцев или изображение лица с места преступления вряд ли приведет к успеху. Объясняется это тем, что алгоритм сопоставления, применяемый в системе регистрации актов гражданского состояния, обычно не рассчитан на работу с данными с места преступления, в отличие от системы поиска в лаборатории судебной экспертизы. Поэтому гражданские базы биометрических данных редко используются при проведении уголовных расследований, и даже если такой поиск проводится в случаях серьезных преступлений или террористических актов, результаты зачастую оказываются крайне низкими. Тем не менее новые технологии и источники данных для

[13] Современная ДНК-технология позволяет всего за час получить профиль ДНК человека по его ротовым мазкам — с помощью полностью автоматизированных устройств, имеющихся в лабораториях, в отделениях полиции и на пограничных пунктах. Это дает возможность вести поиск по базам ДНК с целью установить наличие совпадений образцов, взятых у задержанного или арестованного человека, с образцами, взятыми на месте преступления.

[14] Понятие «место преступления» используется здесь в его самом широком значении и включает, в числе прочего, места, подозреваемых, жертв, свидетелей, а также цифровую и электронную среду.

некоторых модальностей, например изображения лица, могут в будущем повысить эффективность поиска. Кроме того, существует еще один вариант — встроить криминалистические системы распознавания в программы, применяемые в системах регистрации актов гражданского состояния, или присоединить их в качестве приложений.

4.2.2. Криминалистические базы биометрических данных: категории поиска

Рисунок 2. Криминалистические базы биометрических данных — варианты поиска

Существуют четыре основных варианта поиска, применяемых для обеспечения правоохранительной деятельности и при расследовании преступлений, и эти варианты осуществляются в трех конфигурациях (см. рисунок 2).

Поиск в процессе управления идентификационными данными: *вариант поиска 1* — от эталонных данных к эталонным данным

Цель такого поиска — определить, было ли лицо ранее внесено в базу данных. Для этого эталонные данные этого лица сопоставляются со всеми эталонными данными, внесенными в базу. Такой метод чаще всего используется для того, чтобы установить, проходило ли данное лицо по делам оперативного учета органов полиции, имело ли судимость и криминальное прошлое, особенно если этот человек представил ложные сведения о себе. По традиции в этих целях проверяются отпечатки пальцев. У задержанного лица берется — прокатывается[15] — полный набор отпечатков, т.е. отпечатки всех десяти пальцев, которые потом сопоставляются по базе данных с отпечатками пальцев зарегистрированных правонарушителей. Этот метод очень надежен (т.е. имеет очень высокую TAR — см. раздел 4.1), если применялся с использованием современной и высокоэффективной автоматизированной системы идентификации отпечатков пальцев (AFIS), в базе данных которой содержатся только отпечатки пальцев с подтвержденным качеством, соответствующие стандартам и взятые опытными операторами в контролируемых условиях. Подобный поиск обычно проводится автоматизированно, т.е. при минимальном участии человека или вообще без его участия, кроме тех случаев, когда требуется проверить факт совпадения. Это означает, что такой поиск проходит очень быстро. Современные мобильные устройства для сбора данных позволяют сотрудникам правоохранительных органов брать отпечатки пальцев и ладоней у лиц в отдаленном районе или на пункте пограничного контроля и отправлять эти

[15] Кончик каждого пальца прокатывается по считывающему устройству сканера или форме для снятия отпечатков пальцев от одной стороны ногтя до другой, чтобы максимально точно отразить папиллярный узор и его особенности. Кроме того, с пальцев могут быть сняты контрольные оттиски. Такие оттиски получают путем одновременного прикладывания двух больших пальцев вместе и четырех пальцев каждой руки к дактилоскопической карте. Контрольные оттиски делаются для проверки правильности последовательности прокатанных отпечатков пальцев.

данные на центральный сервер для немедленной проверки. Результат, как правило, приходит через несколько минут или даже секунд. Некоторые мобильные устройства имеют автономную базу данных, так что поиск можно проводить на месте, не пересылая данные на удаленный сервер.

Естественно, существует также возможность поиска по идентификационным данным с использованием других биометрических модальностей, например ДНК, изображения лица, радужной оболочки глаза и т.д. Такой поиск может быть проведен и для установления личности умершего или лица, потерявшего память. Основное требование, предъявляемое к любым видам поиска по биометрическим данным, заключается в необходимости получить высококачественные и соответствующие стандартам эталонные данные, чтобы максимально эффективно провести все варианты поиска. Низкое качество эталонных материалов снижает эффективность и точность любых вариантов поиска[16].

Поиск в процессе управления идентификационными данными призван дать ответ на вопрос «Встречались ли мы с вами раньше и кто вы такой?».

Поиск в процессе расследования преступлений: *вариант поиска 2* — от эталонных данных к данным с места преступления — и *вариант поиска 3* — от данных с места преступления к эталонным данным

Протокол такого поиска предполагает двунаправленное взаимодействие между базой эталонных данных и базой данных с места преступления, в которой содержатся криминалистические биометрические данные, полученные на месте преступления, например, следы ДНК (образцы, подлежащие изучению), отпечатки пальцев и ладоней, изображения лица и т.д. Новые собранные эталонные данные, еще не включенные в базу эталонных данных, проверяются по базе данных, полученных на месте преступления, и наоборот, новые данные с места преступления проверяются по базе эталонных данных. Точность такого рода поиска может быть существенно ниже, чем при поиске по идентификационным данным, вследствие того что качество данных, полученных на месте преступления, может различаться.

Поиск в процессе расследования преступлений призван дать ответ на вопросы «Совершили ли вы преступление?», «Связаны ли вы с данным объектом/местом?» и «Был ли с вами кто-либо еще?».

Поиск в случае серийных преступлений/происшествий: *вариант поиска 4* — от данных с места преступления к данным с места преступления

Этот вид поиска позволяет установить связь между местами совершения различных преступлений или преступлений, расследуемых в рамках одного крупного дела, путем выявления и увязывания между собой материалов с разных мест преступления и предоставления следователям по этим делам оперативной информации. Личность человека, оставившего биометрический материал на месте преступления, может быть неизвестна, но установление того факта, что один и тот же человек оставил свой биометрический материал в местах двух и более преступлений или происшествий, может оказать неоценимую помощь следователям и аналитикам оперативных данных. Успешность и точность такого вида поиска в значительной мере определяется качеством данных, собранных на месте преступления, и наличием сопоставимого материала с мест преступлений. Некоторые модальности являются наиболее оптимальными для такого поиска; например, анализ ДНК особенно эффективен для выявления взаимосвязи между преступлениями/происшествиями при расследовании дел разного рода, в том числе террористических актов, убийств и случаев сексуального насилия.

Поиск в случае серийных преступлений/происшествий призван дать ответ на вопрос «Совпадают ли данные с места одного преступления с данными с мест других преступлений/происшествий?».

Примечание. Базы данных, описанные в настоящем разделе, имеют разную величину вероятности ложного недопуска, определяемую типом и качеством биометрических данных, содержащихся в этих базах. Как и во всех других биометрических системах, отсутствие совпадения или отрицательный результат (т.е. случай, когда поиск 1:n не выявил совпадений) означает не то, что в базе данных заведомо

[16] Именно поэтому у всех лиц, арестованных в Соединенном Королевстве по обвинению в преступлениях, связанных с терроризмом, снимается не менее чем по три набора отпечатков пальцев и ладоней, и эта процедура проходит под контролем специалиста по дактилоскопии. Каждый такой набор включает оттиски всех областей гребешковой кожи на руке, т.е. стандартные прокатанные и контрольные оттиски, отпечатки кончиков пальцев, прокатанные оттиски фаланг всех пальцев, оттиск всей поверхности ладони и гипотенара, а также оттиски плантарной поверхности (подошв и пальцев ног). Эта тщательная процедура позволяет получить наиболее полный набор эталонных отпечатков для поиска по AFIS и систематизации, а также крупнейший из существующих набор данных по деталям гребешковой кожи для сопоставления 1:1 со снятыми на месте преступления отпечатками пальцев/ладоней/ступней, прежде всего отпечатков, снятых с кончиков или боковых сторон пальцев или любых участков ладони.

отсутствуют совпадающие данные, а то, что системе не удалось по какой-либо причине обнаружить такие данные.

ДНК[17] — дополнительные категории поиска

Существует также ряд дополнительных специальных методик поиска, применяемых в отношении исследуемых образцов ДНК. Эталонный профиль ДНК получают из некодирующих участков ДНК, и такой профиль используется исключительно для целей идентификации, поскольку он содержит очень мало другой генетической информации. Исследуемые образцы ДНК с места преступления, как правило, содержат гораздо больше генетического материала, и для помощи следствию могут быть применены другие методы извлечения и профилирования ДНК. Вместе с тем эти методы обычно применяются под пристальным надзором со стороны должностных лиц, в обязанности которых входит контроль за соблюдением правовых и этических норм в криминалистике, поскольку использование этих технологий без жесткого контроля может привести к нарушению законов о неприкосновенности частной жизни и персональных данных. Вот лишь некоторые примеры.

Оценка фенотипа — методика выявления генетических физических признаков, например рыжих волос или цвета глаз по следам, оставленным на месте преступления. Хотя возможности этой методики в настоящее время достаточно ограниченны, развитие исследований в сфере ДНК, без сомнения, позволит в будущем расширить спектр фенотипических признаков. Это поможет следователям получить гораздо более подробное «описание» неизвестного подозреваемого по следам ДНК, оставленным на месте преступления.

Поиск по кровному родству — профиль ДНК, составленный на основе анализа следов, оставленных на месте преступления, может не быть идентифицирован, если поиск ведется в базе эталонных данных ДНК. В исключительных случаях по той же базе данных с использованием дополнительного специального программного обеспечения может быть проведен поиск, цель которого — определить, не имеет ли данный профиль значительного сходства с профилем какого-либо близкого кровного родственника (родственников), чьи данные могут быть внесены в систему. В итоге может быть выявлено как относительно небольшое количество, так и многие тысячи ответов — в зависимости от того, насколько редким является данный исследуемый профиль ДНК в сравнении с генетическими профилями всех лиц, внесенных в базу данных.

4.2.3. Криминалистические базы биометрических данных: ограничения и стандарты подготовки заключений

Криминалистические материалы обычно оставляются или фиксируются непреднамеренно, на стадии подготовки преступления или при его совершении, и они могут подвергаться воздействию целого ряда повреждающих факторов, что не позволяет использовать их столь же эффективно, как эталонные данные в системах биометрического поиска. Иногда такие факторы носят общий характер, но многие из них определяются модальностью образца. Вот лишь несколько наиболее часто встречающихся примеров.

Лицо — камеры наружного наблюдения и другие технологии видеозаписи

- *Совместимость угла наклона камер* — камеры наружного наблюдения часто размещаются на возвышении, тогда как фотографии арестованного делаются фронтально на уровне лица. Это затрудняет точное сопоставление двух типов изображений, а иногда делает его невозможным.
- *Освещение и выдержка* — качество снимков, которые делают датчики-камеры, зависит от a) общего освещения данного места и b) таких настроек, как скорость срабатывания затвора, диафрагма и чувствительность.
- *Разрешение камеры* — некоторые камеры имеют очень низкое разрешение, т.е. записывают лишь ограниченное число пикселей, и если камера находится на некотором расстоянии от объекта, то изображение часто получается зернистым и нечетким, особенно если оно было сделано при плохом освещении. В итоге изображение даже при увеличении содержит очень мало пригодных для использования деталей.
- *Сжатие* — устройство записи данных в камере убирает мелкие детали, чтобы можно было сохранить больше изображений более низкого разрешения.

[17] См. также “DNA Database management review and recommendations, 2017, ENSFI DNA Working Group, April 2017”, http://enfsi.eu/wp-content/uploads/2017/09/DNA-databasemanagement-review-and-recommendatations-april-2017.pdf.

- *Черты лица и элементы, закрывающие лицо* — на возможность идентифицировать человека по лицу отрицательно влияют такие факторы, как возраст, выражение лица или неприметельные черты лица, а также внешние помехи, например очки, растительность на лице, головные уборы, шлемы и т.д. (см. раздел 5.2.3.1).

Следы от пальцев или ладоней (известны также как скрытые отпечатки)

- *Достаточность и зона выявления* — в контакт с поверхностью вступает лишь небольшая часть пальца или ладони, и поэтому выявлению поддается лишь относительно небольшое число характерных деталей. Осложнить ситуацию может и плохое качество эталонных отпечатков, поскольку на них могут отсутствовать те небольшие участки пальца, по которым проводится сопоставление с данным следом.
- *Наложение* — два и более следа от пальцев, оставленные на одном и том же участке поверхности, делают крайне сложной задачу визуально отделить один отпечаток от другого.
- *Интерференция* — воздействие вещества, на котором оставлены отпечатки пальцев, может полностью или частично лишить следы от пальцев четкости. Как правило, такие следы остаются либо на поверхности, если они оставлены не на пористом веществе, либо абсорбируются внутрь, будучи оставленными на пористом веществе. Следы, оставленные на поверхности, могут быть подвергнуты повреждению или воздействию окружающей среды. Грязь, загрязняющие вещества или другие помехи также могут лишить четкости или повредить характерные черты следа.
- *Давление* — палец при контакте с поверхностью может подвергаться вертикальному или боковому давлению, что вследствие эластичности кожи может привести к искажению следа.
- *Движение* — при контакте с поверхностью палец может скользить в боковом направлении, что в результате может дать смазанный след, а в некоторых случаях — привести к его искажению или к наложению отпечатков.
- *Ограничения методов проявки* — применение порошка или химических веществ для выявления отпечатков пальцев может не обеспечить четкого выявления всех следов, и в результате отпечатки будут слишком бледными или слишком темными и неконтрастными.

ДНК — биологический и клеточный материал, собранный на месте преступления (известен также как следы преступления)

- *Количество и качество* — как и в случае со следами от пальцев, количество и качество материала ДНК, оставленного на месте преступления, может быть разным, и по этой причине в некоторых случаях совпадение ДНК оценивается не как «полное», а как «частичное». Это происходит в тех случаях, когда материала ДНК недостаточно для определения профиля ДНК, или когда он имеет низкое качество. В этой ситуации, для того чтобы отразить отношение неопределенности, значения вероятности совпадения или отношения правдоподобия соответствующим образом корректируются.
- *Смеси* — на месте преступления может находиться материал ДНК более чем одного человека, и полученный в результате профиль может представлять собой смесь ДНК двух и более лиц. Для интерпретации таких результатов криминалисты применяют статистический анализ, а также, там, где это возможно, помогают отделить ДНК каждого донора и составить их профили. Индивидуальные профили в смеси также могут быть разного качества.
- *Происхождение* — современные лабораторные методы анализа ДНК позволяют составить профиль по ничтожному количеству ДНК на клеточном уровне. Вместе с тем, поскольку ученым сегодня приходится иметь дело со столь малыми образцами, не всегда представляется возможным определить происхождение материала ДНК, найденного на месте преступления, например выделенного из какой-либо конкретной биологической жидкости.
- *Загрязнение* — возможность выявлять и профилировать образцы ДНК, используя для этого столь небольшое количество вещества, напрямую связана с тем, что этот материал по своей природе динамичен, т.е. может быть перенесен от человека к человеку, с одного предмета на другой и с одного места на другое. На месте преступления и в лабораториях необходимо принимать тщательные меры безопасности, чтобы не допустить случайного переноса ДНК в результате действий полиции или криминалистов (см. раздел 5.3).

- *Отрицательное воздействие окружающей среды* — материал ДНК может быть уничтожен, испорчен, либо его свойства могут быть изменены при длительном воздействии неблагоприятных внешних условий, например высоких или низких температур, влажности и загрязнителей.

Соответственно, качество биометрического материала, собранного на месте преступления, колеблется в пределах от низкого, в случае когда отсутствует возможность получить какие-либо биометрические признаки или данные, до весьма высокого, означающего, что биометрический материал имеется в достаточном количестве и обладает четкими признаками, что позволяет сопоставить его с другими биометрическими данными и выявить весьма вероятное совпадение. Относительное качество других биометрических данных, используемых при сопоставлении, будь то эталонный образец или образец с места преступления, также крайне важно для этой процедуры. Возможность выявить ту или иную степень совпадения в процессе сопоставления двух образцов напрямую зависит от их качества. Поэтому эталонные биометрические данные, полученные у лиц в связи с расследованием дел о терроризме, должны, по возможности, соответствовать самым высоким стандартам.

На рисунке 3 представлены этапы изменения качества биометрических образцов и соответствующий им процесс изменения вероятности совпадения — от низкой к высокой. Обычно на биометрическом материале низкого качества получить отрицательный ответ, когда сопоставление показывает, что два биометрических образца не принадлежат одному и тому же человеку, проще, нежели положительный (т.е. совпадение), однако в нижнем сегменте континуума качества оба процесса становятся трудновыполнимыми, и результаты сопоставления могут оказаться неубедительными.

Рисунок 3. Биометрические данные с места преступления — соотношение между качеством биометрического образца и вероятностью совпадения

Критерии внесения в базу данных. Низкокачественные биометрические данные, как правило, не имеют достаточного количества отличительных характеристик, необходимых для проведения поиска, и это означает, что при введении этих данных в систему, например в AFIS, на запрос будет получено непропорционально большое количество ответов, что может в конечном итоге снизить эффективность системы. Это объясняется тем, что система представляет потенциальные совпадения биометрических данных в виде иерархического списка вариантов, как правило, с заранее заданным их количеством, куда чаще всего вносится 10 наиболее вероятных соответствий. Затем оператор проверяет этот список, определяя наличие в нем реальных соответствий. Введение в систему низкокачественных данных может привести к тому, что истинные соответствия в этот список не попадут. Поэтому, принимая решение о внесении биометрического образца в базу данных, необходимо найти баланс между доказательной оперативной и аналитической ценностью каждого образца, с одной стороны, и его техническим и научным качеством — с другой (см. раздел 5.4.2). Если речь идет о нескольких объединенных сетью базах данных, такие пороговые требования к внесению низкокачественных биометрических данных должны соответствовать коллективно выработанным минимальным стандартам, чтобы обеспечить сбалансированную и бесперебойную работу всей сети и не допустить, чтобы партнеры вводили данные, которые могут помешать эффективному ведению поиска.

Исходя из представления о континууме качества биометрических данных, получаемых на месте преступления, криминалисты, специалисты по дактилоскопии и другие эксперты, работающие с криминалистическими материалами, разработали несколько различных методов представления результатов проводимых ими сопоставлений следователям, аналитикам и судам. В широком смысле, к числу таких методов относятся:

- байесовская интерпретация логической вероятности и статистический анализ для проверки гипотез, в том числе отношения вероятности, лежащего в основе сопоставлений профилей ДНК. Следует отметить, что некоторые суды и национальные юрисдикции не принимают определенные варианты этих статистических методов[18];
- вербальные шкалы соответствия, например современные методы сравнения отпечатков пальцев и многие другие криминалистические дисциплины;
- «абсолютные» выводы, например традиционные сравнения отпечатков пальцев.

Это означает, что методы составления заключений по итогам судебно-медицинской экспертизы *в отношении одной и той же модальности* могут быть разными в разных странах и даже в разных юрисдикциях, в зависимости от соответствующих научных, судебных, регуляторных и законодательных требований. Это, в свою очередь, может оказывать влияние на критерии внесения данных в каждую базу, а также на характер получаемых результатов.

Пример из практики 3. Традиционные стандарты работы с отпечатками пальцев

Некоторые страны по-прежнему используют «абсолютный» метод идентификации отпечатков пальцев, представляющий собой традиционную систему, в основе которой лежит бинарный процесс принятия решений по принципу «совпадает — не совпадает» и которая требует наличия заранее определенного минимального стандартного набора характеристик папиллярных узоров (биометрических признаков) для подтверждения совпадения и представления свидетельств в суде. В некоторых странах этот стандарт предусмотрен прецедентным правом. Любое сопоставление отпечатка или следа от пальца с меньшим, нежели предусмотрено действующим стандартом, числом характеристик папиллярных узоров не может быть принято в качестве доказательства. Это очевидным образом может создать трудности в странах, чья правовая система предусматривает принцип полного раскрытия информации, так как суд может потребовать от эксперта дать заключение о сопоставлении отпечатков пальцев, которое представляет интерес для суда (например, может играть значительную роль в деле или быть особенно важным для ответчика), но, по мнению эксперта, не соответствует действующему стандарту и не может быть представлено в суде. Чтобы преодолеть эти ограничения, некоторые другие страны разработали и внедрили в последние десятилетия комплексный нечисловой подход, который не требует наличия минимального количества характеристик папиллярных узоров, а предусматривает строго

[18] Подробнее по этой теме см. ‘Interpreting Evidence: Evaluating Forensic Science in the Courtroom’ by Bernard Robertson & G.A. Vignaux (Wiley ISBN 0471 96026 8) и ‘Introduction to Statistics for Forensic Scientists’ by David Lucy (Wiley ISBN 0-470-02200-0) и ‘Strengthening Forensic Science in the United States: A Path Forward’ by the National Research Council of the National Academies (The National Academies Press ISBN-13: 978-0-309-13135-3).

последовательную и системную оценку деталей папиллярных линий на трех разных уровнях[19]. Этот метод позволяет дать заключение о результатах *любого* сопоставления отпечатков пальцев одним из четырех способов (идентификация, исключение совпадения, недостаточность данных или невозможность дать однозначное заключение на основании имеющихся данных; может также использоваться иная аналогичная терминология) и, таким образом, дает возможность отразить «степень неопределенности» в соответствии с другими областями криминалистики. Вследствие этого при любом международном обмене данными об отпечатках пальцев необходимо учитывать эти различия в составлении научных заключений по одним и тем же модальностям.

В последнее десятилетие в международном сообществе велись серьезные дискуссии и исследования в этой сфере, поскольку многие страны считают целесообразным применять единый метод представления научных заключений, который охватывал бы как традиционные области криминалистики, так и криминалистические экспертизы, связанные с цифровыми и электронными технологиями. Было выдвинуто несколько предложений, однако окончательную модель еще предстоит согласовать, и дискуссии на международном уровне по-прежнему продолжаются. Терроризм представляет собой международную угрозу, и поэтому столь необходимо, чтобы те, кто работает с биометрическими данными и результатами поиска, были в полной мере осведомлены о стандартах составления криминалистических заключений, принятых их партнерами по обмену данными на национальном и международном уровнях. Примером надлежащей практики является также проведение независимой верификации любых результатов, полученных другими партнерскими странами/юрисдикциями, путем проверки выявленных совпадений на предмет их соответствия протоколам криминалистического анализа и стандартам составления заключений, принятым в данной стране (см. раздел 6.4).

4.2.4. Научный анализ: идентичность личности и действия

Существует еще один важный фактор, отличающий стандартное коммерческое биометрическое приложение, например систему доступа в здание на основании биометрических признаков, от криминалистической базы биометрических данных. Обе они способны идентифицировать личность на основании поиска 1:1 или 1:n, однако приложение, используемое в криминалистике, обладает еще одной способностью получать от данных с места преступления доказательства в отношении не только личности, но и действий. Местонахождение, расположение, распределение и ориентация следов преступления могут стать предметом научного анализа и дать дополнительную информацию о времени и последовательности событий, имевших место в ходе инцидента, а также о действиях причастных к нему лиц. Такая дополнительная контекстуальная информация, очевидно, повышает доказательную ценность материалов с места преступления, и следователям и аналитикам, работающим с результатами поиска по криминалистической базе биометрических данных, необходимо понимать и учитывать это в полной мере (см. раздел 6.4).

Примечание. Биографические и связанные с этим данные, собранные при проведении пограничного контроля (см. раздел 6.1.2), могут быть использованы аналогичным образом — в сочетании с биометрическими данными — для получения данных не только о личности, но и о действиях. *Это свидетельствует об эффективности использования биометрических данных с места преступления и данных пограничного контроля и обмена ими для прогнозирования, отслеживания и пресечения террористической деятельности* (см. раздел 6.3.1).

Практические рекомендации к разделу 4

4a Государствам рекомендуется внедрять или более широко применять биометрические системы для идентификации личности отдельных лиц и попыток представлять ложные данные или выдавать себя за другое лицо.

4b Разработка и настройка биометрических систем осуществляются исходя из конкретных служебных требований, предъявляемых к степени их точности, защищенности, количеству пользователей, производительности и эксплуатационной надежности. Поэтому государствам следует тщательно определить собственные требования к таким системам, прежде чем вкладывать деньги в новое биометрическое приложение.

[19] Этот метод известен как ACE-V (анализ, сопоставление, оценка и верификация).

4c Эффективность процедур управления биометрическими идентификационными данными может быть повышена путем их сочетания с поиском по криминалистическим базам биометрических данных, поскольку такое сочетание позволяет создать эффективную общенациональную следственно-аналитическую систему для борьбы с терроризмом и связанной с ним преступной деятельностью.

4d В разных странах применяются разные стандарты и методики представления заключений по результатам криминалистической экспертизы. Соответственно, рекомендуется обучать всех сотрудников, работающих с результатами поиска по криминалистическим базам биометрических данных, пониманию сравнительной ценности этих результатов и возможных ограничений в их использовании.

Справочные материалы к разделу 4

Identity verification The importance of context and continuity of identity, p11-16 Keesing Journal of Documents & Identity, Annual Report Identity Management 2011-2012

В 1995 году Биометрический консорциум при правительстве США дал следующее определение биометрии: «…автоматизированная система распознавания отдельных лиц на основании их поведенческих и биологических характеристик».

Page 1, Biometric Recognition: Challenges and Opportunities, National Research Council, Washington (2010), доступно для скачивания на сайте http://www.nap.edu/openbook.php?record_id=12720&page=1

Jain et al "Biometrics: Personal Identification in Networked Society", Norwell, Mass.: Kluwer Academic Publisher (1999)

Understanding Biometrics Guide (working copy) — Biometrics Institute www.biometricsinstitute.org

PAS 92:2011 Code of Practice for the implementation of a biometric system — British Standards Institute www.bsigroup.com

United Nations Office on Drugs and Crime (UNODC): 'Police: Forensic services and infrastructure' and 'Staff skill requirements and equipment recommendations for forensic science laboratories.' www.unodc.org

UK Forensic Science Regulator Annual Report November 2016 November 2017 — Dr. Gillian Tully

DNA Database management review and recommendations, 2017, ENSFI DNA Working Group, April 2017" http://enfsi.eu/wp-content/uploads/2017/09/DNA-databasemanagement-review-and-recommendatations-april-2017.pdf

Forensic DNA Typing: Biology, Technology and Genetics of STR Markers — John M. Butler. Published by Elsevier Academic Press ISBN-13: 978-0-12-147952-7

Interpreting Evidence: Evaluating Forensic Science in the Courtroom — Bernard Robertson & G.A. Vignaux. Published by Wiley ISBN 0471 96026 8

Introduction to Statistics for Forensic Scientists — David Lucy. Published by Wiley ISBN 0-470-02200-0

Strengthening Forensic Science in the United States: A Path Forward by the National Research Council of the National Academies. Published by The National Academies Press ISBN-13: 978-0-309-13135-3

5. Управление и нормативно-правовое регулирование

С учетом необходимости обеспечить четкость и последовательность содержание нижеследующего раздела, посвященного вопросам управления и нормативно-правового регулирования, распространяется на все разделы настоящего Сборника, и его положения следует считать применимыми ко всем практическим действиям, мерам и рекомендациям, представленным и разъясняемым в данной версии Сборника.

В разделе 5 речь идет о требованиях к управлению биометрической технологией и нормативно-правового требованиях к ней с точки зрения международного права, стандартов в области прав человека, экспертизы этических аспектов, требований к защите данных и права на неприкосновенность частной жизни. Далее следует общий обзор потенциально уязвимых сторон в биометрических системах и рассматриваются некоторые меры контроля, которые можно применять для снижения этих рисков. Затем обсуждаются действующие международные научно-технические стандарты, касающиеся сертификации и аккредитации биометрических приложений, а также систем управления качеством, применяемых для связанных с этим экспертно-криминалистических процедур. В последней части этого раздела рассматриваются требования, предъявляемые к закупке биометрических систем или сетей, предназначенных для борьбы с терроризмом, их техническому обслуживанию и обеспечению ресурсами, и, в частности, ключевые операционные и финансовые решения, которые необходимо принимать в процессе оценки предполагаемого внедрения новой системы или модернизации существующей.

5.1. Международное право, включая стандарты в области прав человека

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. Совет Безопасности и Генеральная Ассамблея Организации Объединенных Наций подчеркивают, что государства обязаны обеспечить, чтобы любые меры, принимаемые в целях борьбы с терроризмом, соответствовали всем их обязательствам по международному праву, и прежде всего международным стандартам в области прав человека, беженскому праву и гуманитарному праву. Уважение прав человека и принципа верховенства закона сопряжено с эффективной контртеррористической деятельностью и является необходимым условием успешной борьбы с терроризмом[20].

Очевидно, что сфера применения прав человека различна в разных государствах-членах. Некоторые государства не являются участниками некоторых универсальных документов по правам человека, а другие являются участниками региональных документов по правам человека[21], отличающихся друг от друга в определенных аспектах. Государства-члены отличаются друг от друга и по масштабам включения международных стандартов в области прав человека в национальное законодательство. Кроме того, некоторые государства при ратификации этих документов или присоединении к ним делали оговорки или принимали заявления, ограничивающие их готовность соблюдать те или иные договорные обязательства.

Совет Безопасности в своей резолюции 2396 (2017) 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. При разработке систем сбора биометрических данных важно предусматривать гарантии в отношении защиты данных и соблюдения стандартов прав человека[22], обращая особое внимание на необходимость ответственно подходить к использованию любых систем, создаваемых для сбора и хранения информации (в том числе биометрических данных) о детях, и к обмену такой информацией в соответствии с национальным и международным правом, прежде всего положениями Конвенции Организации Объединенных Наций о правах ребенка (КПР) (1989 год).

---

[20] См., например, резолюции 1373 (2001), 1624 (2005), 2178 (2014) и 2396 (2017) Совета Безопасности; резолюции A/RES/68/276 и A/70/L.55 Генеральной Ассамблеи.

[21] См., например, публикацию Агентства ЕС по основным правам ‘Under Watchful Eyes — Biometrics, EU-IT Systems & Fundamental Rights, http://fra.europa.eu/en/publication/2018/biometrics-rights-protection.

[22] S/2015/975, пункт 8; S/2015/939, принцип 15 (e).

Применение биометрии, не нарушающее права человека

Государства все чаще используют биометрические технологии как важное средство борьбы с терроризмом. Идентификация по голосу, сканирование радужной оболочки глаза, отпечатки пальцев, ДНК, сканирование тела и распознание человека по походке — это лишь некоторые примеры цифровых технологий, разрабатываемых и применяемых в целях борьбы с терроризмом. Эти технологии порождают сложные правовые и политические проблемы, касающиеся как контртеррористической деятельности государств, так и их обязательств в области прав человека. Притом что биометрические системы могут быть законным средством для идентификации лиц, подозреваемых в причастности к терроризму, широкие технические возможности и быстрое развитие таких технологий требуют повышенного внимания, поскольку речь здесь идет о защите прав человека, в том числе о праве на неприкосновенность частной жизни, хотя и не только о нем. Согласно статье 17 Международного пакта о гражданских и политических правах, никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию; каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств. Совет Организации Объединенных Наций по правам человека признал, что «нарушения или ущемление права на неприкосновенность частной жизни могут негативно сказываться на осуществлении других прав человека, в том числе права свободно выражать свои мнения и беспрепятственно придерживаться их и права на свободу мирных собраний и ассоциации…»[23]. Хотя согласно международному праву право на неприкосновенность частной жизни не является абсолютным, признано, что любое вмешательство в осуществление этого права должно соответствовать принципам законности, соразмерности и необходимости. Кроме того, разрешаемое государством вмешательство может совершаться только на основании закона, который должен в свою очередь соответствовать положениям, целям и задачам Пакта и являться обоснованным в конкретных обстоятельствах[24]. Любое такое вмешательство не должно также являться дискриминацией по признаку расы, языка, религии, национального или социального происхождения, политических и иных убеждений или по любым иным мотивам, предусмотренным международным правом[25].

Специальный докладчик Организации Объединенных Наций по вопросу о праве на неприкосновенность частной жизни отметил, что в ряде стран мира установлено всеобщее основополагающее право на достойную жизнь и свободное, беспрепятственное развитие личности и нарушения права на неприкосновенность частной жизни могут негативно сказаться на этом праве[26]. В преамбулах к Всеобщей декларации прав человека и Международному пакту о гражданских и политических правах говорится, что признание достоинства, присущего всем членам человеческой семьи, и равных и неотъемлемых их прав является основой свободы, справедливости и всеобщего мира[27]. Неправомерное использование биометрических данных может создавать угрозу для этих прав. Злоупотребление такими данными может также создавать серьезные риски для прав на надлежащую правовую процедуру, в том числе на право на презумпцию невиновности и другие права, связанные с рассмотрением уголовного обвинения[28]. Кроме того, массовый сбор таких данных без соблюдения принципов необходимости и соразмерности может сам по себе являться нарушением права на неприкосновенность частной жизни[29].

Для предупреждения ненадлежащего использования биометрических данных государствам необходимо рассмотреть возможность пересмотра их законодательства о защите персональных данных и внесении в него корректив, отражающих современные виды применения усовершенствованных биометрических технологий. Государствам следует также пересмотреть свое законодательство для решения непростых задач, возникающих в связи с дальнейшим развитием биометрических технологий. Основанный на принципах соблюдения прав человека подход к использованию биометрических технологий должен предусматривать применение процессуальных гарантий и эффективный контроль за

---

[23] Резолюция A/HRC/RES/34/7 (2017) Совета по правам человека.

[24] Комитет по правам человека, замечание общего порядка № 16: Статья 17 (Право на неприкосновенность частной жизни), пункты 3 и 4.

[25] Международный пакт о гражданских и политических правах, статьи 2 (1) и 26.

[26] Доклад Специального докладчика по вопросу о праве на неприкосновенность частной жизни, A/HRC/31/64 (2016).

[27] Всеобщая декларация прав человека и Международный пакт о гражданских и политических правах, преамбула.

[28] Международный пакт о гражданских и политических правах, статьи 9, 14.

[29] Международный пакт о гражданских и политических правах, статья 2 (3).

их соблюдением[30]. Это предполагает, в числе прочего, создание соответствующих независимых надзорных органов, которые осуществляли бы контроль за деятельностью государственных учреждений, уполномоченных предоставлять эффективные средства правовой защиты в случаях нарушений, а также создание независимых надзорных органов, которые обеспечивали бы соблюдение государственными учреждениями и частным сектором законов о неприкосновенности частной жизни и о защите персональных данных[31].

5.1.2. Этические аспекты и биометрия

Технологии, подобные биометрии, порождают особые проблемы из-за разрыва между внедрением технологических инноваций и принятием законов, регулирующих эти технологии. Соответственно, некоторые государства создают органы по экспертизе этических аспектов и другие надзорные органы, чтобы в упреждающем порядке изучить такие новые технологии и приложения и вырабатывать рекомендации относительно нынешнего и возможного будущего законодательства, правительственной политики и стратегического планирования. В состав этих органов обычно входят высококвалифицированные ведущие специалисты, представляющие гражданское общество, а также могут входить представители государственного и частного секторов, научно-технические работники, деятели науки и рядовые граждане. Подобные группы по этическому надзору стремятся рассматривать вопросы с широкой точки зрения, в том числе потенциальные последствия применения биометрических технологий для отдельных групп и сообществ, прежде всего в том, что касается расовой принадлежности, пола, возраста, религиозных убеждений и сексуальной ориентации.

Примером подобного подхода может служить нижеследующий случай из практики.

Пример из практики 4. Британская группа по этическим аспектам биометрии и криминалистики[32]

Эта группа возникла на базе ранее существовавшей Национальной группы по этическим аспектам работы с ДНК, созданной для надзора за методами и тактикой научной работы с первой в мире базой данных о ДНК. Сегодня в сферу ведения группы входят криминалистика в целом, а также биометрические технологии. Группа рассматривает каждую новую проблему в широких рамках права, этики и социальной политики. Группа придерживается перечисленных ниже руководящих принципов.

---

[30] Комитет по правам человека в своем замечании общего порядка № 16 (1988) подчеркнул, что государства должны принимать эффективные меры к тому, чтобы информация, касающаяся личной жизни какого-либо лица, не попадала в руки лиц, которые не имеют разрешения на ее получение, обработку и использование, и чтобы такая информация никогда не использовалась в целях, не совместимых с Международным пактом о гражданских и политических правах. Эффективная защита должна предусматривать для каждого лица возможность удостовериться в ясной форме, содержатся ли в автоматизированных файлах персональные данные, и если содержатся, то какие и с какой целью, а также соответствующее право потребовать исправления неправильных данных или их изъятия. Каждое лицо должно иметь также возможность выяснить, какие государственные органы или частные лица или органы контролируют или могут контролировать их файлы. См. http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en.

[31] Резолюция 45/95 (1990) Генеральной Ассамблеи о руководящих принципах регламентации компьютеризированных картотек, содержащих данные личного характера; Общий регламент Европейского союза по защите данных, 2018 год, статья 51 (Надзорный орган).

[32] https://www.gov.uk/government/publications/biometrics-and-forensics-ethics-group

Руководящие принципы ***В отношении биометрических и криминалистических процедур***	**Руководящие принципы** ***Осуществление принципов***
Процедуры следует применять в целях укрепления общественной безопасности и ради общественного блага Процедуры следует применять в целях продвижения правосудия При осуществлении процедур необходимо обеспечить соблюдение прав человека отдельных лиц и групп лиц При осуществлении процедур необходимо обеспечить уважение достоинства каждого человека Необходимо, чтобы процедуры, по мере возможности, обеспечивали соблюдение права на частную и семейную жизнь, если это не противоречит законной цели системы уголовного правосудия по защите граждан от причинения вреда Необходимо использовать последние достижения науки и техники для обеспечения скорейшего снятия подозрений с невиновных, защиты потерпевших и возмещения им ущерба, а также содействия в отправлении уголовного правосудия Процедуры должны быть основаны на убедительных доказательствах	Беспристрастность — процедуры должны осуществляться непредвзято и без необоснованной дискриминации Пропорциональность — обеспечение баланса между правами отдельного лица и общественным благом Открытость и прозрачность Необходимость создания систем выявления ошибок Необходимость контроля качества Необходимость публичной подотчетности Обеспечение, в соответствующих случаях, независимого надзора Необходимость предоставлять надлежащую информацию и, в соответствующих случаях, получать согласие лиц, чьи данные или образцы предполагается получить

Группа определила также принципы сбора и обработки данных:

- данные следует собирать, хранить и использовать только в конкретных и законных целях;
- сбор, хранение и использование данных следует осуществлять в соответствии с требованиями законодательства;
- необходимо принимать меры к обеспечению точности, защищенности и целостности собранных, хранимых и используемых данных;
- необходимо, чтобы процедуры были надежными, соответствовали международным стандартам и осуществлялись подготовленным персоналом;
- вторжение в частную жизнь должно быть минимальным;
- необходимо учитывать интересы вторичных субъектов данных (имеются в виду лица, чьи интересы могут быть затронуты данными, собранными в отношении других лиц, например члены семьи).

Терроризм угрожает многим государствам, и в ответ на это правоохранительные органы быстрыми темпами разрабатывают и внедряют новые технологии в сфере биометрии и криминалистики, которые позволили бы усилить безопасность и расширить возможности проведения расследований. Группы по этическому надзору могут сыграть свою роль в этой работе, поскольку они имеют возможности давать информированные комментарии по вопросам подготовки или внедрения любых новых технологий или стратегий. Это не отменяет необходимости в последующем принятии законодательства, но может помочь не допустить внедрения новых методов и практик, если они не сбалансированы или в них нет необходимости. Эта работа может также обратить внимание законодателей на актуальность и значимость рассматриваемого вопроса.

Стандарты и примеры взаимодействия между биометрией и этикой

На сегодняшний день не существует единых международных и даже национальных стандартов этичного получения и использования биометрических данных, равно как и большинства новых технологий. Международная организация по стандартизации (ИСО) изложила разработанные ею стандарты в документе «Юридические и социологические соображения по применению. Часть 1. Общее руководство» (ISO/IEC TR 24714:2008) и в Руководящих указаниях 71:2014, где речь идет об этических аспектах, а также в Руководящих указаниях 71 о стандартах обеспечения доступности для лиц преклонного возраста и инвалидов.

Вопрос о применении биометрии в соответствии с этическими нормами затрагивает и гуманитарную сферу. Существует ряд программ, в рамках которых использование биометрии принесло немало пользы. Так, например, Управление Верховного комиссара Организации Объединенных Наций по делам беженцев (УВКБ ООН) с 2002 года применяет биометрические системы в своих программах и все шире осуществляет регистрацию на основании биометрических данных. Применяемая УВКБ ООН в глобальном масштабе биометрическая технология — Система биометрической аутентификации (БИМС) — дает организации возможность гарантировать уникальность каждой регистрации и проверять, что помощь, предоставляемая ею в разных формах (включая продовольствие, денежные пособия, меры по защите или переселению и т.п.), доходит до надлежащих получателей. Есть и другие примеры, когда идентификация на основании биометрических данных позволяла свести к минимуму махинации на выборах или финансовые злоупотребления — два потенциальных фактора дестабилизации, способные вызвать беспорядки или привести к росту терроризма.

УВКБ ООН рекомендует также проводить биометрическую регистрацию лиц, ходатайствующих о предоставлении убежища, в качестве составного элемента систем въезда, учитывающих необходимость обеспечения защиты. Это предполагает разработку необходимых мер обеспечения безопасности для предупреждения возможного проникновения уголовных преступников или лиц, принадлежащих к террористическим и экстремистским организациям. Передовая практика в этой сфере предполагает: 1) осуществление надлежащей регистрации, в том числе с использованием биометрических данных, сотрудниками пограничных служб, прошедшими подготовку по соответствующим вопросам обеспечения безопасности, средствам защиты прав беженцев и прав человека; и 2) направление лиц, обращающихся за международной защитой, для прохождения процедур получения убежища. Чтобы не создавать рисков для соискателей убежища/беженцев, необходимо сделать общим принципом, что биометрические и другие персональные данные таких лиц могут передаваться странам их происхождения только по завершении процедуры предоставления убежища и обеспечении их защиты. Это относится также к третьим странам в ситуациях, когда вероятно возникновение риска для эффективной защиты искателя убежища или беженца[33].

5.2. Защита данных и право на неприкосновенность частной жизни

Биометрическая технология — мощный инструмент борьбы с терроризмом в мировом масштабе. Она позволяет выявлять и пресекать террористическую деятельность и защищать население от неизбирательных нападений. Однако основой этой технологии является сбор, хранение и использование персональных данных. Как указывалось выше, биометрические данные должны быть защищены законом, а их обработка должна осуществляться без нарушения основных прав человека, таких как право на неприкосновенность частной жизни.

5.2.1. Правовые критерии регистрации данных и стандарты защиты данных

Совет Безопасности Организации Объединенных Наций в своей резолюции 1373 (2001) отметил тесную связь между международным терроризмом и транснациональной организованной преступностью, запрещенными наркотиками, отмыванием денег, незаконным оборотом оружия. В той же резолюции Совет постановил, что государства должны предотвращать передвижение террористов или террористических групп с помощью эффективного пограничного контроля и контроля за выдачей документов, удостоверяющих личность, и проездных документов, а также с помощью мер предупреждения фальсификации, подделки или незаконного использования документов, удостоверяющих личность, и проездных документов.

[33] См. пункт 17 раздела Е документа УВКБ ООН «Решение проблем безопасности без отрицательных последствий для защиты беженцев», http://www.refworld.org/docid/5672aed34.html.

Для противодействия этим отношениям крайне важно создать достаточный и эффективный потенциал борьбы с терроризмом во всех государствах-членах[34]. Одним из важнейших инструментов создания такого потенциала является использование биометрии[35]. Поскольку применяемые террористами тактические приемы часто включают кражу документов или идентификационных данных, использование биометрии служит ценным инструментом восстановления идентификационных данных лиц, пострадавших от их кражи (см. раздел 5.3.6).

Для создания биометрической системы, которая была бы эффективной и в то же время соответствующей законам по защите данных и обеспечивающей соблюдение права на неприкосновенность частной жизни, необходимо принять во внимание перечисленные ниже факторы.

Обеспечение качественной регистрации данных — необходимо установить высокие стандарты качества регистрации данных, с тем чтобы обеспечить точную регистрацию и сопоставление биометрических данных в самых разных условиях, в том числе в отдаленных районах, на пограничных пропускных пунктах или в аэропортах, где все больше возрастает потребность в ускоренной обработке данных пассажиров при поддержании надлежащего уровня точности. Когда речь идет о детях или юридически несовершеннолетних, сопровождающих родителей или путешествующих в одиночестве, следует учесть возможность изменения некоторых биометрических данных детей по мере их взросления. Кроме того, Совет Безопасности Организации Объединенных Наций в своей резолюции 2396 (2017) подчеркивает, что с детьми необходимо обращаться таким образом, чтобы соблюдались их права и уважалось их человеческое достоинство, в соответствии с применимыми нормами международного права.

Законодательство о неприкосновенности частной жизни — правоохранительные органы могут ограничивать право на неприкосновенность частной жизни в том случае, если принимаемые ими меры являются необходимыми и соразмерными и соответствуют нормам международного права в области прав человека. Например, персональные данные подозреваемых и их сообщников можно использовать в чрезвычайных ситуациях, когда можно не учитывать необходимость соблюдения основных принципов конфиденциальности, таких как осознанное согласие или сбор сопутствующих личных данных. Тем не менее в большинстве случаев соблюдение таких принципов конфиденциальности, как осознанное согласие, сбор и использование персональных данных только для заявленных целей, а также право на исправление неточных или заведомо ложных сведений, следует считать требованием по умолчанию. Кроме того, следует документировать и регистрировать в журнале причины отказа от выполнения этих требований по умолчанию. Для обеспечения высокого уровня безопасности доступ операторов к этим системам должен также контролироваться при помощи биометрических данных.

Финансирование терроризма — биометрические данные могут быть использованы в рамках системы мер, направленных на предотвращение связанных с терроризмом мошенничества, кражи идентификационных данных и финансовых операций и на уменьшение этих угроз в финансовой системе. Таким образом, одним из эффективных вариантов является использование биометрических данных для контроля доступа к транзакциям. Немало преимуществ с точки зрения местного населения и охраны правопорядка у национальных программ защиты потребителей от связанных с терроризмом случаев мошенничества и кражи идентификационных данных[36].

Международные стандарты защиты персональных данных — стандарты защиты персональных данных должны соответствовать международным стандартам, нежели менее распространенным вариантам или техническим стандартам, которые могут зависеть от таких факторов, как лоббистские усилия местных компаний, или даже основываться на системах, бесплатно предоставленных оказывающими помощь донорами. В качестве начальных критериев при выборе системы следует использовать соответствующие стандарты Международной организации по стандартизации (ИСО), Международной организации гражданской авиации (ИКАО) и Всемирной таможенной организации, подкрепленные разработанными Институтом биометрии принципами неприкосновенности частной жизни и контрольным перечнем вопросов для оценки воздействия на неприкосновенность частной жизни[37].

---

[34] См. также резолюции 2195 (2014) и 2178 (2014) Совета Безопасности.

[35] Резолюция 2396 (2017) Совета Безопасности ООН и его предыдущая резолюция 2178 (2014).

[36] См. перечень инструментов по борьбе с отмыванием денег и иными формами мошенничества, приводимый на веб-сайте Международного валютного фонда www.imf.org.

[37] См. www.biometricsinstitute.org.

Приемлемость доказательств — следует принять меры к тому, чтобы использование всех биометрических и персональных данных было ограничено целями, для которых эти данные были собраны. Это позволит также обеспечить приемлемость данных, собранных для включения в базы данных, для уголовного преследования. При этом, в частности, следует предусмотреть меры по обеспечению содействия со стороны отрасли ИКТ, при условии что для такого содействия была создана правовая основа.

Интерпретация результатов биометрии — правоохранительные органы, производящие задержание террористов или осуществляющие их уголовное преследование, должны быть осведомлены о риске неправильной интерпретации результатов, полученных из баз биометрических данных, например при частичном совпадении ДНК или неубедительном совпадении изображения лица вследствие воздействия внешних факторов при фиксации изображения лица с низким качеством в плохих условиях. В таких ситуациях до принятия каких-либо мер абсолютно необходимо провести контекстный анализ (см. раздел 7).

5.2.2. Политика сохранения или удаления данных

Это — одна из сфер, в которой процедуры, связанные с охраной правопорядка и борьбой с терроризмом, должны осуществляться в соответствии с нормами международного права в области прав человека, в том числе права на неприкосновенность частной жизни. Например, право лица на просмотр файла со своими персональными данными либо на их корректировку или подачу запроса об удалении данных (эти права часто закреплены в законах о неприкосновенности частной жизни, например в Общем регламенте Европейского союза по защите данных — ОРЗД)[38] может также быть ограничено необходимостью обеспечить защиту свидетелей или конфиденциальность текущего расследования.

В мире существуют самые разные стратегии в отношении сохранения данных, особенно данных лиц, арестованных в рамках расследований, проводимых правоохранительными органами. Во многих странах биометрические данные лиц, осужденных за преступления, сохраняются в течение жизни правонарушителя, но при этом не существует единого стандарта в отношении биометрических данных лиц, подозреваемых в совершении преступлений или арестованных за совершение преступлений, но не осужденных.

Надлежащей практикой считается хранение биометрических данных отдельно от соответствующих биографических данных. У лиц, пострадавших от кражи идентификационных данных (в результате преступной или террористической деятельности), может возникнуть необходимость скорейшего восстановления их украденных или использованных неправомерным образом идентификационных данных. При разработке системы необходимо будет составить план по восстановлению связи между биометрическими и биографическими данными в случае возникновения подобной ситуации. Для этого можно разместить в массиве биометрических данных один сегмент метаданных в виде уникального идентификационного номера. Но процесс восстановления связи должен быть защищенным, для того чтобы во всех обстоятельствах обеспечить целостность системы и структуры данных. Необходимо также применять надежный протокол обеспечения безопасности, в соответствии с которым:

- сотрудник, получающий доступ к системе, должен занимать в организации должность высокого уровня;
- для получения доступа к системе он должен использовать свои биометрические данные;
- его доступ к системе должен быть официально зафиксирован;
- должна быть официально зафиксирована причина, по которой сотрудник запрашивает доступ к системе.

Безопасность может быть дополнительно усилена за счет увеличения в организации числа сотрудников, занимающихся выдачей или отзывом разрешений на доступ к системе. Это обеспечит ротацию персонала, выполняющего эти обязанности, и создаст дополнительный уровень безопасности.

[38] Общий регламент Европейского союза по защите данных, 2018 год, статья 7 (Согласие), статья 17 (Право на уничтожение данных), статья 15 (Право на доступ к данным).

5.2.3. Обработка данных

Организация, занимающаяся обработкой данной, должна назначить контролера данных, который будет отвечать за руководство всеми мероприятиями по обработке данных, включая их сбор, хранение, использование и удаление. Контролер данных продолжает нести ответственность даже в том случае, если функция по обработке данных передается на подряд другим сторонам.

Наиболее всеобъемлющее законодательство о неприкосновенности частной жизни требует от органов власти, занимающихся сбором персональных данных, гарантировать запрет на обработку или хранение этих данных в странах, где законодательством о неприкосновенности частной жизни предусмотрен более низкий уровень защиты, чем в стране, где был произведен сбор данных.

С любыми независимыми поставщиками или операторами данных необходимо заключать контракты, обязывающие их поддерживать очень высокий уровень безопасности и предусматривающие внешние аудиторские проверки, осуществляемые ведомством-заказчиком, и наказания за несоблюдение предписанных контрактом требований к безопасности и конфиденциальности.

5.2.4. Обмен данными

Организация Объединенных Наций в ряде заявлений подчеркнула необходимость сотрудничества государств в области совершенствования законодательства в целях уголовного преследования террористов, в особенности иностранных боевиков-террористов, обеспечивая при этом защиту прав человека и неприкосновенность частной жизни в соответствии с законом[39]. Для обмена персональными данными, в том числе биометрическими данными, в режиме реального времени также необходимо сотрудничество между государственными органами и между государствами, позволяющее обеспечить совместимость используемых платформ и форматов[40].

При обмене персональными данными террористов или лиц, подозреваемых в террористической деятельности, необходим высокий уровень доверия по целому ряду вопросов, в том числе относительно использования предоставляемых данных, их точности и контекста, объема и типа данных, которые могут быть предметом обмена. В основе механизмов обмена данными должны лежать официальные соглашения, заключенные между всеми участвующими сторонами.

Есть и иные факторы, которые необходимо будет учитывать в рамках процесса обмена данными. К их числу относятся требование о том, чтобы запрос на получение персональных данных основывался на твердом подозрении в причастности к террористической деятельности, подробно изложенные критерии доказанности, а также прояснение вопроса о том, не были ли эти данные получены в деморализующих условиях, что имеет для многих стран важнейшее доказательственное значение.

Как правило, применяются изложенные ниже принципы.

1. Обмен персональными данными, в том числе биометрическими, должен быть утвержден в установленном законом порядке на национальном уровне и регламентироваться четкой нормативно-правовой базой, распространяющейся на органы, которые отправляют и получают эти данные, как на национальном, так и на международном уровне.
2. Использование данных должно ограничиваться утвержденными целями, для которых они были получены.
3. Обмен данными должен осуществляться только с заслуживающими доверия получателями[41]. Поскольку изложенный в разделе 5.2.3 принцип распространяется и на обмен данными,

---

[39] Резолюция 2322 (2016) Совета Безопасности ООН о международном сотрудничестве и резолюция 2396 (2017) Совета Безопасности ООН об ужесточении мер борьбы с угрозами, создаваемыми возвращающимися иностранными боевиками-террористами.

[40] Резолюция 2178 (2014) Совета Безопасности ООН и Мадридская декларация министров иностранных дел, принятая 28 июля 2015 года на специальном совещании Контртеррористического комитета Совета Безопасности.

[41] Примерами соглашений об обмене персональными данными между заслуживающими доверия получателями служат, например, соглашения об обмене данными о регистрируемых преступлениях между Отделом регистрации преступлений (ACRO) Соединенного Королевства и Федеральным бюро расследований США либо полицейскими и иммиграционными властями других стран Европейского союза или глобальной защищенной полицейской системой связи Интерпола I-24/7, подкрепленной базой данных Интерпола о похищенных и утерянных проездных документах и поисковой системой для выявления связанных с уведомлениями проездных документов.

персональные данные не должны направляться в страны, где уровень защиты неприкосновенности частной жизни ниже, чем в стране, отправляющей данные.

4. Чтобы не создавать рисков для искателей убежища/беженцев (согласно разделу 5.1.2), биометрические и другие персональные данные таких лиц могут передаваться странам их происхождения только по завершении процедуры предоставления убежища и обеспечении их защиты (см. также пример из практики 10, раздел 6 — пункт *Решение проблемы беженцев*).

5.2.5. Предотвращение противоправного использования данных

С противоправным использованием данных связаны по крайней мере два затрагиваемых здесь ключевых вопроса.

Первый — это абсолютная необходимость обеспечить защиту всех персональных данных, включая биометрические, от несанкционированного доступа и противоправного использования. Речь идет как о внешних угрозах, так и о внутренних злоупотреблениях со стороны персонала, имеющего доступ к данным.

Второй — это необходимость обеспечить точность предоставляемых персональных данных, а также гарантировать, что эти данные предоставляются в надлежащем контексте и не в злонамеренных целях. Это приобретает особую важность, в случае если правительство или иная сторона будет пытаться внести данные своих политических оппонентов в списки подозреваемых, с тем чтобы нарушить их основные права.

5.2.6. Обеспечение безопасности и проверка данных

Каждая организация должна назначить контролера данных, занимающего достаточно высокий пост, обладающего достаточной профессиональной подготовкой и профессиональным опытом, который будет нести ответственность за сбор, использование и перемещение всех персональных данных, включая биометрические.

В его основные обязанности входят принятие стратегических решений и разработка стандартных операционных процедур. На этапе разработки системы такое лицо также должно принять решение относительно выбора наиболее подходящей для использования биометрической модальности или модальностей.

Чтобы обеспечить эффективность любых стратегий и практических мер обеспечения неприкосновенности частной жизни и безопасности, необходимо как минимум принять решения по следующим вопросам, независимо от того, использовались ли какие-либо биометрические технологии:

- Была ли проведена оценка воздействия на неприкосновенность частной жизни[42] до внедрения новой бизнес-практики или новой технологии?
- Существуют ли программы и процедуры профессиональной подготовки и повышения осведомленности, способствующие поддержанию надлежащей культуры обеспечения неприкосновенности частной жизни и защиты прав человека, а также расширению рабочих знаний о биометрии среди всех сотрудников, эксплуатирующих систему?
- Применяются ли методы шифрования или преобразования данных на важнейших этапах сбора, хранения, использования персональных данных, в том числе биометрических, и обмена ими?
- Существуют ли процедуры строгого контроля и учета доступа, предписывающие лицам, получающим доступ к конфиденциальным данным, представлять собственные биометрические данные?
- Существуют ли документированные процедуры, определяющие механизмы отчетности и меры по исправлению ситуации в случае нарушения неприкосновенности частной жизни и безопасности?

[42] Оценка воздействия на неприкосновенность частной жизни (PIA) является частью концепции «проектируемой конфиденциальности», используемой для управления данными в государственных и коммерческих организациях. Процедура проведения PIA обеспечивает соответствие правовым и регуляторным нормам неприкосновенности частной жизни посредством выявления потенциальных рисков и разработки стратегий смягчения этих рисков и управления ими.

- Проводятся ли регулярные испытания и аудиторские проверки, призванные подтвердить применение практических мер обеспечения неприкосновенности частной жизни и безопасности, а также их надежность и эффективность?
- Существует ли официальная процедура документирования и решения проблем, выявленных в результате регулярной аудиторской проверки?
- Проводятся ли регулярные выборочные проверки подлинности и целостности персональных данных, хранящихся в системе?

Рекомендации для контролеров данных и организаций, в которых они работают, содержатся в ряде международных стандартов и руководств[43].

При проверке подлинности собранных данных, в том числе биометрических, необходимо следовать надлежащей процедуре в целях соблюдения прав человека, в том числе права на неприкосновенность частной жизни, но при этом обеспечивать полное соблюдение судебных требований, предъявляемых к лицам, в отношении которых вынесен обвинительный приговор, или, например, к процедуре выдачи. В отношении процедуры выдачи такие требования могут быть более жесткими в одних странах, чем в других, особенно в части критериев доказательности или проведения допроса.

Правоохранительные органы и органы пограничного контроля должны руководствоваться ключевым принципом, предусматривающим наличие специальных групп аналитиков, обладающих достаточными навыками и ресурсами для получения точных и имеющих практическую ценность результатов. Это помогает при проведении мониторинга до и после совершения террористических актов, а также при сборе приемлемых доказательств, включая такие биометрические данные, как ДНК, отпечатки пальцев, изображения лиц и записи голосов. В данном случае следует использовать весь спектр методов поиска и сбора биометрических данных.

5.2.7. Надзор

Противоправное использование персональных данных (как по ошибке, так и в злонамеренных целях) может привести к неблагоприятным правовым последствиям для отдельных лиц или нанести им иной ущерб. В частности, это касается списков подозреваемых лиц и других механизмов оповещения.

Следует проявлять осторожность при внесении подозреваемых террористов или уголовных преступников в списки подозреваемых лиц. Прежде чем вносить данные какого-либо лица в этот список, необходимо провести тщательную всестороннюю проверку для оценки оснований для включения и проверки подлинности всех запросов. Данные, содержащиеся в списках подозреваемых лиц, должны подвергаться регулярной проверке в целях подтверждения их действенности и актуальности.

Аналогичным образом, в соответствии с международным правом в области прав человека и законодательством по защите неприкосновенности частной жизни субъекты данных должны иметь право на обжалование включения своих данных в любой подобный список. Органы власти, составляющим списки подозреваемых лиц, должны обнародовать информацию о праве на обжалование и апелляцию и о существовании механизмов подачи жалоб.

При осуществлении процедуры включения данных в списки на правоохранительные органы, органы борьбы с терроризмом и органы пограничного контроля налагается обязанность собирать, хранить и анализировать данные лиц, подозреваемых в терроризме, и их сообщников, а также данные о моделях их поведения, таких как перелеты, финансовые операции и изменение места проживания. Однако необходимо принять меры к тому, чтобы хранение сведений о подозреваемых лицах и их сообщниках осуществлялось на конфиденциальной и санкционированной правовой основе, с тем чтобы не допустить неправомерного лишения свободы или судебного преследования.

Необходимо обеспечить надежные гарантии от произвольного сбора, хранения и использования персональных данных, в том числе создать механизмы надзора с привлечением независимого органа. В некоторых государствах, возможно, уже существуют органы надзора за неприкосновенностью частной жизни, которые могли бы исполнять эти функции в рамках существующих или расширенных

[43] Резолюция 45/95 (1990) Генеральной Ассамблеи о руководящих принципах регламентации компьютеризованных картотек, содержащих данные личного характера, и руководство по вопросам неприкосновенности биометрических данных (*Biometric Privacy Guidelines*), разработанное Институтом биометрии для международного использования, www.biometricsinstitute.org.

обязанностей. Если же в настоящее время в государстве нет такого органа, его следует создать для исполнения этой важнейшей роли.

В частности, чрезвычайно важно, чтобы учрежденные в законном порядке надзорные механизмы были независимыми, эффективными и беспристрастными. Они должны иметь необходимые полномочия для мониторинга и оценки надежности гарантий защиты биометрических данных, в том числе в связи с международным обменом этими данными. Физические лица должны иметь возможность связываться с надзорным механизмом для получения информации о своих данных и для подачи жалобы, если они считают, что их права оказываются под угрозой. Субъектам данных следует, по мере возможности, предоставлять в четкой и доступной форме информацию относительно обработки. В законе следует предусмотреть надлежащие средства правовой защиты, если при обработке биометрических данных нарушаются права человека, в том числе права на неприкосновенность личной жизни.

5.3. Управление рисками в системе

5.3.1. Введение

Управление 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.

В приложениях контртеррористического характера, как правило, используются комплексные биометрические системы, включающие ряд компонентов ИТ и предусматривающие взаимодействие со средой сбора данных и интерпретацию человеком. Таким образом, возникает ситуация многоаспектного риска со множеством потенциальных точек отказа системы, особенно если учесть, что лица, занимающиеся терроризмом, обладают высокой мотивацией, а зачастую обеспечены достаточными ресурсами для обхода контроля служб безопасности.

Применение в целях борьбы с терроризмом систем, не имеющих надлежащих механизмов управления рисками, может привести к возникновению иллюзорной уверенности в эффективности этих систем. Возможными последствиями этого могут стать ошибочная идентификация разыскиваемых лиц, утечка сугубо конфиденциальной информации о списках подозреваемых лиц или внедрение вредоносных кодов.

Известные или подозреваемые террористы нередко путешествуют под чужим именем или по подложным документам. С точки зрения управления рисками важно обеспечить корректное использование традиционных систем сопоставления биографических данных (см. раздел 6.1.5). В целях уменьшения этого риска национальные органы пограничного контроля могут использовать верификацию биометрических данных и поиск по спискам подозреваемых лиц (см. раздел 6.2.2).

Конфигурация биометрической системы в высшей степени зависит от конкретных условий. Например, каждый аэропорт отличается от других в экологическом аспекте, а также по характеру поведения пассажиров и их демографическому профилю. Это обусловливает наличие различных видов риска, требующих применения различных стратегий смягчения. Тем не менее есть одна чрезвычайно важная стратегия смягчения риска, которая подходит для использования в любых условиях: проведение специалистами-тестировщиками регулярных активных тестов на проникновение в систему в целях своевременного выявления рисков и понимания их характера.

Управление рисками — это специализированный вид деятельности, регламентируемый как международными, так и национальными стандартами (см. перечень справочных материалов в конце данного раздела).

Важнейшим фактором для каждого пользователя является бесперебойное функционирование системы, и неотъемлемой частью стандартных операционных процедур для любой биометрической системы должны быть протоколы действий в чрезвычайных обстоятельствах. Поэтому, в случае если в какой-либо части системы произошел сбой и система не в состоянии обеспечить нормальное обслуживание, необходимо принять одну или несколько неотложных мер для осуществления временного обслуживания. Это может быть выполнение персоналом определенных операций вручную (например, в случае отказа автоматических биометрических турникетов паспортного контроля сотрудники органов

пограничного контроля выполняют проверку паспортов вручную) или переход на использование резервной системы или массива резервных компонентов[44].

5.3.2. Уязвимые места и новые угрозы

Для целей анализа все угрозы в биометрических приложениях, используемых для борьбы с терроризмом, были распределены по следующим основным категориям.

- *Общие информационные технологии*. Все прикладные технологии, используемые для управления базами данных, безопасной передачи информации, проверки действий пользователей и профилактики заражения вирусами. В этой сфере следует опираться на передовой опыт обеспечения безопасности ИТ в государственных системах.
- *Биометрические датчики и внешняя среда*. Вид используемой технологии и связанные с ней риски. Например, использование фальшивых отпечатков пальцев, темных очков или технологий, изменяющих голос.
- *Механизмы сопоставления биометрических данных*. Конфигурация механизмов сопоставления, в том числе настройка порогового уровня, выявление случаев представления подозрительных идентификаторов и управление списками подозреваемых лиц.
- *Контроль со стороны человека*. Для любой биометрической системы характерен тот или иной показатель вероятности ложного допуска и ложного недопуска; это прежде всего относится к поиску, проводимому в процессе расследования преступления, поскольку качество зарегистрированных биометрических данных может быть неодинаковым (см. раздел 4). Изучение и оценку этих случаев ложного допуска и недопуска должны проводить соответствующим образом обученные операторы. Неправильная обработка данных потенциально может привести к ошибочным задержаниям, применению неэффективных методов работы или, наоборот, к упущению особо опасных лиц, внесенных в списки подозреваемых.

Области угроз	Ответственные лица	Последствия	Примеры мер по смягчению рисков
Общие информационные технологии	Руководители служб информационной безопасности	Рассекречивание списков подозреваемых лиц, нарушение безопасности системы, подмена совпадений. Кража биометрических шаблонов, которые могут быть использованы для реконструкции биометрических признаков	Обеспечение безопасности связи, антивирусы, брандмауэры (отказ в обслуживании), управление списками биографических данных подозреваемых лиц, безопасное взаимодействие с внешними системами. Аннулируемые биометрические данные
Биометрические датчики и внешняя среда	Компании-поставщики/системные интеграторы	Лица, внесенные в списки подозреваемых, способны избежать обнаружения, введя в заблуждение датчики	Совокупность внешних условий, выявление случаев представления подозрительных идентификаторов, фильтрация по качеству. Алгоритмы борьбы со спуфингом (выявление спуфинг-атак)

[44] Хорошим примером может служить избыточный массив независимых дисков (RAID) — технология, часто используемая в автоматизированных системах идентификации отпечатков пальцев (AFIS). Она дает возможность сконфигурировать диски небольшой емкости на сервере в крупный массив, позволяющий повысить производительность и безопасность, а также обеспечить резервирование в комплексе серверов. Большинству правоохранительных органов — пользователей систем AFIS необходимо, чтобы система функционировала круглосуточно и круглогодично, поэтому для них неприемлемо отключение системы на продолжительный период для технического обслуживания, обновления или ремонта. Таким образом, гибкое использование дублированного RAID позволяет обеспечить непрерывное функционирование системы: в случае отказа нескольких дисков или их вывода из рабочего режима данные сохранятся на активных дисках, что позволит обеспечить бесперебойное обслуживание пользователя.

Области угроз	Ответственные лица	Последствия	Примеры мер по смягчению рисков
Механизмы сопоставления биометрических данных	Компании-поставщики/системные интеграторы/служба информационной безопасности	Лица, внесенные в списки подозреваемых, способны избежать обнаружения	Настройка системы, контроль качества регистрируемых данных, надлежащее управление серверами баз данных. Использование мультимодальных биометрических систем вместо одной биометрической модальности
Контроль со стороны человека	Государственные службы безопасности/операторы	Ошибочные задержания, неэффективные методы работы, упущение особо опасных лиц, внесенных в списки подозреваемых	Образование, профессиональная подготовка и аккредитация, проведение аудиторских проверок, разработка пользовательского интерфейса и надлежащей терминологии

Таблица 1

5.3.3. Классификация угроз по модальностям

Биометрические системы сопряжены со сложным комплексом угроз, который продолжает расширяться по мере дальнейшего внедрения биометрических технологий. Создание всеобъемлющей классификации всех уязвимостей и рисков в этой области выходит за рамки данного документа, однако они описаны в стандарте ИСО/МЭК 30107-2_2017 [1], а некоторые конкретные примеры приводятся в документе, предназначенном для служб пограничного контроля [2].

К числу широко распространенных биометрических модальностей, используемых для целей борьбы с терроризмом, относятся следующие.

Лицо. Лицо — это наиболее распространенный и доступный объект для получения биометрических данных при помощи систем сбора данных с близкого расстояния или дистанционно, однако для этих систем характерны определенные проблемы и технические ограничения, способные привести к получению низкокачественных изображений лица. Такие изображения существенно влияют на вероятность корректного распознавания (или, наоборот, на число случаев, когда система дает ложный доступ). Повлиять на это может как качество фотографии, использованной для внесения данных в список подозреваемых лиц, так и фотографии, сделанной камерой. В справочном документе [3] можно ознакомиться с примерами повышения эффективности распознавания лица при помощи систем наблюдения. К числу конкретных параметров, влияющих на качество изображения, относятся освещение, поза, положение камеры, выражение лица, головные уборы, очки, бороды, разрешение (выраженное в пикселях расстояние между глазами) и возраст.

К часто встречающимся уязвимостям, связанным с изображением лица, в частности, относятся:

- *мошенничество с участием внешне похожих лиц.* Документ, удостоверяющий личность, используется разыскиваемым лицом, внешне схожим с подлинным владельцем этого документа. Таким образом, в случае обнаружения лицо, внесенное в список подозреваемых, может заявить, что в действительности не является тем, кого разыскивают;
- *маски.* Используются усовершенствованные латексные маски, которые трудно обнаружить при беглом наблюдении;
- *грим.* Правильное использование грима может скрыть черты лица и помочь избежать обнаружения, при этом лицо будет выглядеть естественно для человека-наблюдателя;
- *очки.* Темные очки или очки в массивной оправе могут скрыть важные черты лица, используемые для распознавания;
- *поведение.* Если объект подозревает, что за ним следят, он может смотреть на экран мобильного телефона или вниз, препятствуя получению качественного изображения;

- *трансформация изображений (морфинг)*. Слияние биометрических образцов (например, изображений лиц), принадлежащих двум и более донорам, с тем, чтобы обеспечить успешную верификацию любого из таких доноров на основе «преобразованных» идентификационных данных.

Отпечатки пальцев. Дактилоскопическую биометрию применяют правоохранительные органы во всем мире; соответственно, существует множество баз данных и списков подозреваемых лиц с шаблонами отпечатков пальцев (см. раздел 4). К часто встречающимся уязвимостям дактилоскопических биометрических систем, в частности, относятся:

- *фальшивые пальцы.* Использование фальшивых пальцев, сделанных из веществ, имитирующих свойства кожи. Они могут надеваться отдельно на каждый палец или быть частями перчаток, надеваемых на обе руки;
- *преднамеренное повреждение.* Если объект подозревает, что находится под наблюдением, он может попытаться испортить свои отпечатки пальцев, используя химические вещества или абразивные материалы или применяя иные методы;
- *посмертные отпечатки пальцев.* Используя отпечатки пальцев умерших людей, террористы создают идентификационные данные, чтобы открывать счета в банках и совершать финансовые операции в целях финансирования своей деятельности.

Радужная оболочка глаза. Распознавание по радужной оболочке глаза является точной и надежной биометрической модальностью. Радужная оболочка глаза не изменяется со временем и с трудом поддается подделке. В настоящее время ведутся масштабные научно-исследовательские и опытно-конструкторские работы, направленные на повышение устойчивости систем распознания по радужной оболочке глаза к спуфингу и по их внедрению в сферу пограничного контроля в качестве альтернативной/дополнительной модальности. К числу уязвимостей этих систем относятся:

- использование *косметических контактных линз* с напечатанной радужной оболочкой;
- использование высококачественных изображений лиц, доступных в интернете, для получения *распечатанных изображений глаз*;
- максимально возможное *расширение зрачков*. В этом случае сканер может не распознать радужную оболочку глаза (когда алгоритм сопоставления применяется к тому же глазу с существенно отличающимся размером зрачка, эффективность распознания радужной оболочки снижается);
- *матричные контактные глазные линзы* с поддельным изображением радужной оболочки. Вследствие этого система сканирования радужной оболочки не сможет распознать радужную оболочку в своей базе данных;
- *склеральные контактные линзы с нарисованной на них радужной оболочкой*. Эти линзы полностью закрывают видимую область глазного яблока, и внешний вид глаз у человека, надевшего эти линзы, окажется совершенно иным;
- *хирургическое вживление по-другому окрашенной радужной оболочки* поверх настоящей радужной оболочки глаза человека. Хотя многие люди используют этот вид хирургического вмешательства только для того, чтобы изменить свой цвет глаз, лицо, желающее скрыть свою идентичность, также может использовать эту процедуру;
- при проведении аутентификации для сопоставления необходим эталонный шаблон, который должен быть под рукой, что создает для злоумышленника возможность похитить шаблоны и проводить дальнейшие атаки.

Голос. Технология идентификации голоса может использоваться для того, чтобы отслеживать телефонные звонки и предупреждать об обнаружении подозреваемых лиц. В целом технология идентификация голоса обеспечивает невысокую точность результатов, когда ее применяют в отношении больших объемов переданных данных или больших баз данных (особенно при передаче данных по нескольким телефонным линиям). Тем не менее эта технология может оказаться эффективной, если применять ее в тех случаях, когда количество отслеживаемых телефонных звонков и количество лиц в списке подозреваемых оказывается относительно ограниченным.

К часто встречающимся уязвимостям систем распознания голоса, в частности, относятся:

- *устройства, изменяющие голос.* Существует ряд приложений для смартфонов, позволяющих изменять голос;
- *синтезированная речь.* Одним из новых векторов угроз является применение устройств, которые могут быть настроены на голос, т.е. напечатанное сообщение может быть прочитано синтезированным голосом с естественными интонациями.

5.3.4. Качество данных для регистрации

Независимо от использованной модальности, низкокачественные биометрические данные могут оказаться неподходящими для использования в списке подозреваемых лиц. При использовании недостаточно качественных биометрических данных возникает высокая вероятность пропуска истинных совпадений и появления большого числа случаев ложного допуска. Оценка и регулирование качества биометрических данных является важным аспектом обеспечения точности биометрической системы. У каждой модальности имеются собственные параметры качества: например, для лица такими параметрами являются освещение, поза и головные уборы. Любой фактор, способствующий ухудшению качества или маскировке биометрических данных в процессе регистрации, повлияет на поисковые возможности системы и на ее способность к сопоставлению данных. Определения параметров качества содержатся в ряде стандартов ИСО (см. раздел 5.4).

5.3.5. Пропускная способность и управление ею

Пропускная способность системы естественным образом зависит от объема компьютерных ресурсов, используемых для проведения сопоставления и обработки данных. Сопоставление биометрических данных зачастую является дорогостоящим вычислительным процессом, особенно если речь идет об обширных списках подозреваемых лиц. Одним из важнейших ограничительных факторов в сфере сопоставления биометрических данных являются людские ресурсы. Для рассмотрения каждого случая сопоставления данных требуется подготовленный оператор, способный провести оценку. Это означает, что, например, даже при использовании системы распознания лиц с хорошо настроенным сбалансированным пороговым показателем число случаев ложного допуска, требующих рассмотрения в напряженной обстановке, может быть значительным. Крайне важно учитывать эти требования при рассмотрении бюджета, принимая во внимание не только стоимость первоначального развертывания системы, но и ее дальнейшую эксплуатацию.

5.3.6. Кража идентификационных данных

В общем смысле, кража идентификационных данных представляет собой несанкционированное получение персональных данных физического лица, т.е. имени, даты рождения, адреса и т.д., в целях совершения преступных деяний, в частности мошенничества, связанного с использованием похищенных данных для получения фиктивного займа, кредитной карты или приобретения дорогостоящих товаров. Кража идентификационных данных, которыми являются биометрические данные, поднимает ряд важных проблем, поскольку биометрические признаки, как правило, остаются неизменными на протяжении всей жизни человека и их невозможно сменить так же легко, как личный идентификационный код (ПИН-код) или пароль. Кража биометрических данных может представлять собой кражу фактических физических биометрических данных человека, например создание копии отпечатков пальцев или маски его лица, или кражу биометрического шаблона, хранящегося в приложении или базе данных. В целях борьбы с этими рисками был разработан ряд важных мер, и к числу основных таких мер, в частности, относятся перечисленные ниже.

Распознавание живой материи. В устройства для сбора биометрических данных встраиваются различные датчики, способные проникнуть за пределы вещества представленных биометрических данных и отличить кожу живого человека от искусственной подделки.

Аннулируемые биометрические данные. При регистрации биометрических данных в системе характерные признаки этих данных подвергаются намеренному неоднократному искажению. Если впоследствии шаблон повреждается или похищается, его заменяют шаблоном тех же самых, но искаженных биометрических данных, поэтому похищенный шаблон сразу же становится недействительным. Таким образом, одни и те же биометрические данные могут быть использованы в различных приложениях, но шаблоны везде будут разными. «Оригинальные», не искаженные

биометрические признаки никогда не подвергаются регистрации, что способствует более эффективной защите неприкосновенности частной жизни и предоставлению пользователям более надежных гарантий.

Следует отметить, что, в случае когда биометрические данные используются вместе с идентификационными документами (например, паспортами), риск кражи идентификационных данных сводится к минимуму, поскольку, даже если биометрические данные будут украдены или скопированы, злоумышленнику все равно придется предъявить действительный документ, который, если это понадобится, можно сделать недействительным. Биометрические данные, так же как изображение лица, могут быть собраны заинтересованными лицами скрытно или получены из источников в интернете. Поэтому органы власти, использующие лицо в качестве биометрической модальности в официальных документах, должны учесть риск подобных краж и разработать надлежащие меры для его смягчения.

5.4. Международные стандарты

5.4.1. Технические операционные стандарты

Очень важно обеспечить, чтобы любая биометрическая система, предназначенная для борьбы с терроризмом, была безопасной, неизменно надежной и отвечала конкретным бизнес-требованиям пользователя. В основе данных требований лежат следующие ключевые факторы:

- испытание системы для обеспечения ее соответствия текущим и будущим функциональным характеристикам и параметрам;
- безопасность операционной среды и сети;
- правовая оценка и оценка воздействия на неприкосновенность частной жизни;
- управление рисками в комплексной системе;
- доказуемая компетентность оператора;
- обработка данных и обеспечение целостности всех элементов системы, таких как устройства для сбора биометрических данных, регистрация данных в системе и обеспечение документов, подтверждающих идентичность, хранение и извлечение данных, показатели эффективности сопоставления и вероятность ошибок, любые другие небиометрические метаданные;
- надежность программного обеспечения и аппаратных средств;
- совместимость — передача данных и обмен данными с другими системами;
- разработка интерфейса «человек–компьютер» — простого в использовании для 1) нахождения и регистрации субъектов данных в системе и 2) работы системных операторов, включая набор инструментов, рабочее место, эргономичные аспекты и внешние условия.

Существует множество международных, региональных и национальных стандартов, охватывающих важные элементы и периферийные функции. Владельцы, пользователи и потребители биометрических систем ориентируются на эти стандарты, чтобы обеспечить гарантированно эффективную работу их приложений на протяжении всего эксплуатационного цикла в соответствии с функциональными характеристиками, заложенными производителем. Они также используют данные стандарты для обеспечения надежности таких процессов, как закупка (см. раздел 5.4) и техническое обслуживание и обновление биометрической системы, особенно если она представляет собой часть обширной национальной или международной сети, осуществляющей обмен данными. Партнеры или потенциальные партнеры едва ли согласятся участвовать в работе такой сети в том случае, если другие ее участники эксплуатируют свои биометрические системы не в соответствии с национальными или международными стандартами.

Международная организация по стандартизации[45] (ИСО) разрабатывает и публикует стандарты по широкому кругу отраслей, включая биометрию и криминалистику. ИСО — это всемирное объединение национальных органов по стандартизации из 162 стран, которые вносят вклад в разработку стандартов посредством участия в работе различных профильных комитетов. Другие страны могут присоединиться к ИСО в качестве ассоциированных членов или членов-подписчиков для получения информации о стандартах.

[45] http://www.iso.org

Кроме того, существуют два совместных комитета ИСО и Международной электротехнической комиссии[46] (МЭК), которые разрабатывают стандарты и проводят оценки соответствия (ОС) для всей электрической, электронной и связанной с этим продукции. Оценка соответствия дает потенциальному покупателю, возможно не до конца разбирающемуся в тонкостях системы или продукта, гарантию того, что данный продукт соответствует техническим стандартам и стандартам безопасности или другим указанным критериям. Существуют три вида ОС. Поставщик проводит *оценку соответствия первой стороной*, пользователь — *оценку соответствия второй стороной*, но наиболее надежной является *оценка соответствия третьей стороной*, проводимая независимыми органами. Этот процесс носит название сертификации, поскольку, как правило, после успешного проведения оценки продукту или услуге выдается сертификат, который служит подтверждением того, что продукт или услуга соответствует определенной спецификации или стандарту ИСО/МЭК.

Региональные органы также могут разрабатывать стандарты в целях унификации систем и методов работы в группе стран. Например, Европейский комитет по стандартизации[47] (ЕКС) объединяет национальные органы по стандартизации из 34 европейских стран. В рамках Комитета действует специальная Рабочая группа по биометрическим данным (РГ-18), которая приводит разработанные международными или национальными организациями стандарты в соответствие с европейскими требованиями в таких областях, как неприкосновенность частной жизни и законодательство о защите данных.

Некоторые стандарты разрабатываются на национальном уровне соответствующими организациями для своих стран: например, в США действуют такие организации, как Американский национальный институт стандартов (АНИС) и Национальный институт стандартов и технологий (НИСТ), которые разрабатывают стандарты, применяемые в криминалистике и в связанных с нею биометрических приложениях. Многие страны широко применяют стандарты НИСТ в таких важных областях, как электронная передача отпечатков пальцев по сетям. НИСТ также проводит сравнительные испытания и составляет рейтинги имеющихся на рынке алгоритмов поиска и сопоставления биометрических данных для применения к другим биометрическим модальностям, таким как лицо и радужная оболочка глаза[48]. Благодаря этому потенциальные покупатели систем сопоставления биометрических данных могут получить объективные сведения об относительной эффективности алгоритмов, используемых конкурирующими производителями на международном рынке.

5.4.2. Научные стандарты эксплуатации и процедуры управления качеством

Помимо технических стандартов и программ сертификации, предназначенных для биометрических систем, существуют стандарты ИСО для криминалистических процедур, например стандарт ИСО/МЭК 17025:2017 «Общие требования к компетентности испытательных и калибровочных лабораторий». В данном стандарте устанавливаются процедуры и требования к компетентности при проведении научных испытаний и/или калибровки, включая отбор образцов. В нем рассматриваются вопросы управления процессами, а также компетентности и беспристрастности научных работников и эффективности используемых ими методов. В целях обеспечения непрерывного усовершенствования деятельности и аккредитации лабораторий стандарт предусматривает проведение как внутренних аудитов и испытаний, осуществляемых самой лабораторией, так и внешних аудитов и аттестационных испытаний, осуществляемых при участии и под контролем внешних аккредитационных органов. Эти регулярные независимые инспекционные проверки проводятся для того, чтобы определить, отвечает ли лаборатория надлежащим стандартам, требуемым для получения или сохранения аккредитации в соответствии с ИСО 17025:2017. Аккредитация подтверждает, что лаборатории располагают полнофункциональной системой управления качеством (СУК) и обладают достаточной компетентностью для систематического проведения научных испытаний и калибровки в соответствии со стандартом.

СУК осуществляет регулярный обзор всех факторов, способствующих эффективному функционированию лаборатории, а также, что особенно важно, всех случаев несоблюдения установленных требований. Для выявления первопричин любого несоблюдения используются процедуры корректирующих действий, а в целях недопущения повторения подобных ситуаций разрабатываются превентивные меры. В рамках внутренних управленческих обзоров регулярно проводится оценка

[46] http://www.iec.ch

[47] https://www.cen.eu

[48] http://www.nist.gov

эффективности работы лаборатории с использованием всеобъемлющего контрольного списка организационных, ресурсных, процедурных и управленческих требований, разработанных на основе руководства по качеству для лаборатории.

Существуют стандарты, которые могут применяться в других областях криминалистики, например при проведении расследований на месте преступления (например, ИСО 17020:2012). Таким образом, большое значение имеет возможность применения в операциях по борьбе с терроризмом подхода, основанного на использовании стандартов и охватывающего все криминалистические процедуры от места преступления до зала суда, в том числе:

- управление местом преступления и его осмотр, включая криминалистические и биометрические стратегии (см. раздел 6.4.2), оценки интерпретации, координацию ресурсов, методы отбора проб, процедуры недопущения загрязнения, упаковочные материалы, допросы подозреваемых, опросы свидетелей и потерпевших;
- лабораторные процедуры, включая отбор проб, проведение анализа, управление базой данных, компетентность персонала и представление отчетов о полученных результатах;
- представление доказательств в суде — протоколы показаний привлеченных экспертов, беспристрастность и методы представления доказательств.

5.5. Управление закупками и ресурсами

5.5.1. Закупки

Правительства стран должны разработать собственную нормативно-правовую базу и критерии отбора, чтобы контролировать процесс закупки товаров и услуг. Вместе с тем имеется ряд важных моментов, которые следует учитывать при оценке потребности в биометрической системе, а также некоторые конкретные аспекты, связанные с приобретением приложений, используемых для борьбы с угрозой терроризма:

Бизнес-требования. В бизнес-плане необходимо четко указать преимущества и причины использования биометрических систем вместо альтернативных способов распознавания и аутентификации. Преимущества следует оценить в сравнении с потенциальными недостатками, такими как стоимость, технические уязвимости, возможные возражения и сопротивление со стороны общественности/клиентов, опасения этического характера и другие угрозы, указанные в процедуре оценки рисков. Необходимо тщательно оценить количество пользователей и мощности базы данных в настоящем и в будущем, чтобы убедиться в том, что система сумеет справиться с ожидаемыми нагрузками, особенно в периоды наивысшего спроса (см. раздел 5.3.5).

Защита неприкосновенности частной жизни и защита данных (см. раздел 5.1). Использование биометрической системы для идентификации известных и подозреваемых террористов возможно только при условии соблюдения прав физических лиц на неприкосновенность их частной жизни и защиту персональных данных в соответствии с национальным и международным правом. Биометрические системы могут допускать ошибки, выражающиеся в неверной идентификации людей либо неспособности их идентифицировать, что влечет за собой значительные репутационные риски для владельца (владельцев) данных. Необходимо тщательно изучить эти аспекты на этапе разработки любого биометрического приложения и внедрить надлежащие процедуры для разрешения и смягчения подобных ситуаций, если они возникнут.

Примечание. Ресурсы, необходимые для расширения функционала существующего органа по надзору за неприкосновенностью частной жизни или для создания нового органа (см. раздел 5.2.7), следует включать в бюджет любой национальной или региональной политики или проектного плана по разработке биометрических систем, используемых для борьбы с терроризмом.

Безопасность. Любая часть биометрической системы или биометрической сети, в которой используются данные, имеющие отношение к террористам или террористическим актам, может стать объектом внешней электронной/кибератаки, физического нападения, внутреннего вмешательства или саботажа в результате неправомерных действий персонала. Следовательно, необходимо создать многоуровневую систему безопасности для защиты операционной среды, аппаратных средств, программного обеспечения, сети связи и хранимых данных. Кроме того, следует также уделить внимание вопросам проверки персонала, работающего с системой, и удостовериться, что он не может стать

объектом какого-либо принуждения со стороны террористов или их пособников. Также необходимо проводить регулярные аудиторские проверки на предмет выявления случаев коррупции среди персонала и фактов злоупотреблений. В рамках общей стратегии безопасности необходимо также выявлять и предотвращать другие угрозы, такие как спуфинг-атаки (см. раздел 5.2).

Эффективность. Биометрические приложения, используемые для борьбы с терроризмом, должны функционировать с наивысшей точностью, т.е. с чрезвычайно низкой частотой ошибок, сохраняя при этом приемлемую пропускную способность. Жизнь множества людей может оказаться под угрозой в том случае, если система по каким-либо причинам и на каком-либо этапе не сумеет идентифицировать террориста. Для достижения и поддержания высокой эффективности и периодического обновления биометрической системы, скорее всего, понадобится значительный объем финансирования на протяжении всего срока ее эксплуатации. Ввиду наличия высокого риска процедуры обработки исключений также должны быть всесторонними и тщательными, с тем чтобы помешать террористам намеренно избегать биометрических проверок и проходить их там, где используются потенциально менее эффективные резервные системы.

Биометрическая модальность. Решение о выборе одной или нескольких конкретных модальностей может приниматься в зависимости от перечисленных ниже факторов.

- Доступность и функциональность. Основной вопрос, связанный с принятием решения в отношении закупки, заключается в том, использовать ли в приложении одну биометрическую модальность или применять мультимодальный подход. Выбранная модальность или модальности должны быть пригодны для решения задач сопоставления — верификации (1:1) и идентификации (1:n). Закупка и эксплуатация мономодальных систем, как правило, обходятся дешевле, однако такие системы не могут охватить все население. Например, значительное количество людей может оказаться не в состоянии пройти регистрацию в системе отпечатков пальцев, поскольку у них покалечены или отсутствуют пальцы или кисти рук либо кожа на руках повреждена в связи с их профессиональной деятельностью, например у людей, работающих с химическими веществами или занимающимися иными видами ручного труда, способными лишить четкости, исказить или уничтожить гребешковую кожу на пальцах и ладонях. Если биометрическое приложение применяется для регистрации как можно большего числа людей, то предпочтительнее использовать мультимодальную систему (например, с такими модальностями, как отпечатки пальцев и радужная оболочка глаза), поскольку с ее помощью можно будет собрать биометрические данные у большей части целевой группы населения. Аналогичное решение по закупке необходимо принять и в отношении функциональности системы, т.е. целесообразно ли приобрести биометрическое приложение, предназначенное для выполнения лишь одной функции, например полицейскую систему учета отпечатков пальцев уголовных преступников, или лучше повысить ценность инвестиций, создав многофункциональную сеть, включающую, например, приложения по регистрации преступлений, базы данных о преступлениях и приложения пограничного контроля? Можно даже расширить функции и модальности, если национальное законодательство допускает такую возможность, с тем чтобы в стране действовала единая биометрическая система. Некоторые страны применяют такой мультимодальный и многофункциональный подход, обеспечивающий экономию за счет масштаба, оптимизацию численности персонала за счет объединения сходных функций и наличие в национальной системе лишь одной структуры управления и руководства.
- Совместимость и техническая перспективность модальностей. При выборе наилучшей модальности для приложения, используемого для борьбы с терроризмом, ключевым фактором будет возможность получения и обмена данными с национальными или международными партнерами в целях выявления потенциальных террористов. Например, страны могут создать региональную сеть и обмениваться данными об отпечатках пальцах всех лиц, подающих заявки на получение визы и пересекающих их границы. Поэтому каждая страна, желающая присоединиться к данной сети и воспользоваться ее преимуществами, должна будет использовать отпечатки пальцев в своей биометрической системе регистрации лиц, подающих заявки на получение виз, даже если изначально в обосновании делового предложения по каким-либо причинам было рекомендовано использовать другую модальность. Также можно расширить эту сеть за счет рассмотрения возможности использования нескольких модальностей, поскольку они также являются биометрическими данными, обычно собираемыми на местах преступлений, и могут помочь при проведении перекрестного поиска в целях борьбы с терроризмом. Например, предпочтение будет отдаваться использованию таких

модальностей, как отпечатки пальцев и лицо, а не радужная оболочка глаза или рисунок вен на тыльной стороне ладони.

- Сбор и регистрация данных. Например, что выгоднее, чтобы субъект находился в контакте с устройством для сбора данных или в непосредственной близости к этому устройству либо в данной оперативной обстановке оптимальным вариантом будет дистанционный сбор данных?
- Приемлемость и пропускная способность. Некоторые биометрические модальности могут стать предметом предвзятых суждений клиентов, вызывать обоснованную обеспокоенность или даже общественное неприятие: например, отпечатки пальцев нередко ассоциируются с преступным миром из-за своей исторической роли в охране правопорядка. Некоторым модальностям может быть отдано предпочтение из-за того, что они позволяют использовать более быстрые и простые процедуры сбора и регистрации данных. Этот фактор зачастую влияет на выбор приложений, которые используются для работы с большим количеством клиентов на регулярной основе, например в пунктах пограничного контроля.

5.5.2. Управление ресурсами

Закупка важной, крупномасштабной биометрической системы требует значительных капиталовложений для приобретения необходимых аппаратных средств и программного обеспечения и создания надлежащей безопасной рабочей среды, т.е. пунктов регистрации и сбора данных, серверных помещений, помещений для операторов и т.д. Кроме того, для некоторых систем могут потребоваться расходы на наем и обучение персонала, а если эксплуатация осуществляется на основе стандартов, — на периодическую аккредитацию.

После установки системы и успешного проведения приемочных испытаний проводится регулярное техническое обслуживание, а также периодическое обновление программного обеспечения и системы безопасности, которые финансируются за счет средств годового бюджета. Помимо этих расходов, средства годовых доходов будут в основном расходоваться на оплату труда персонала и на поддержание повседневного и эффективного функционирования системы. Как правило, биометрические системы должны функционировать круглосуточно и круглогодично с минимальным простоем.

Благодаря современным рыночно ориентированным исследованиям и разработкам в области биометрических технологий во всем мире непрерывно появляются новые варианты программного обеспечения, происходит стремительное обновление возможностей систем. Срок эксплуатации многих биометрических систем превышает 20 лет, поэтому во избежание их устаревания потребуется их многократная модернизация. Без регулярного технического обслуживания и обновления в течение всего срока его службы надежность любого биометрического приложения может значительно снизиться или оно может полностью выйти из строя.

В процедурах закупок и планирования необходимо также учитывать другие потребности, которые возникнут в будущем: например, для того чтобы справиться с возросшим спросом, необходимо будет наращивать вычислительную мощность, а следовательно, и емкость запоминающего устройства базы данных. Кроме того, может возникнуть производственная необходимость в обеспечении связи и операционной совместимости с другими системами или базами данных. Любые из этих усовершенствований потребуют в будущем дополнительного финансирования, однако этих средств может не оказаться в наличии, если впоследствии бюджет подвергнется сокращению либо приоритет будет отдан другим конкурирующим потребностям. Поэтому было бы целесообразно заранее учесть эти аспекты и потребности на этапе планирования и предусмотреть в новых системах максимум таких факторов. При разработке приложений следует предусмотреть резерв вычислительных мощностей и памяти либо заблаговременно рассчитать стоимость этих обновлений и согласовать возможность их осуществления в закупочных контрактах. Если сетевые возможности учитываются уже на начальном этапе, то новую систему можно также снабдить функционалом связи и операционной совместимости с другими системами. Гораздо дешевле создавать подобные интерфейсы на этапе разработки системы, чем включать их в систему позднее, когда они могут помешать ее функционированию и, возможно, потребовать установки или реконфигурации компонентов и каналов связи в обеих/всех системах.

Практические рекомендации к разделу 5

5a Государствам необходимо принять основанный на принципе соблюдения прав человека подход к использованию биометрической технологии в целях борьбы с терроризмом, предусматривающий применение процессуальных гарантий и эффективный надзор за их соблюдением. Это предполагает, в числе прочего, создание соответствующих независимых надзорных органов или расширение полномочий уже существующих органов, которые осуществляли бы контроль за выполнением соответствующего законодательства по защите неприкосновенности частной жизни и предоставлением эффективной правовой помощи в случае нарушений. Кроме того, необходимо разработать процедуру экспертизы этических аспектов, которая должна быть включена в процесс разработки всех национальных стратегий и директивных решений, касающихся использования биометрических данных для целей борьбы с терроризмом.

5b При применении биометрических технологий для борьбы с международным терроризмом и связанными с ним преступлениями надлежит обеспечить соблюдение основных прав всех граждан на неприкосновенность частной жизни и законную защиту персональных данных, включая биометрические данные.

5c Биометрические системы могут испытывать сбои в работе и подвергаться различным видам преднамеренных атак. В связи с этим государствам рекомендуется проводить регулярные оценки рисков на всех стадиях работы их биометрических систем в целях смягчения существующих или возникающих угроз.

5d Государствам рекомендуется эксплуатировать свои биометрические системы в соответствии с международными техническими стандартами и стремиться обеспечить официальную аккредитацию своих криминалистических процедур и процедур управления качеством в соответствии с международными научными стандартами. Эти меры не только послужат надежным основанием для эффективной обработки биометрических данных, но и будут способствовать укреплению доверия со стороны международных партнеров, которые могут выразить желание обмениваться биометрическими данными.

5e Закупки биометрических систем требуют долгосрочного стратегического планирования, учитывающего как текущие, так и будущие потребности в ресурсах, поэтому государствам следует обратить внимание на следующие аспекты:

- первоначальные капиталовложения для приобретения и испытания системы;
- стабильные ежегодные расходы на персонал и на техническое обслуживание системы, а также на обновление программного обеспечения и системы безопасности;
- размер бюджета, емкость базы данных и вычислительная мощность, которые потребуются в течение всего срока службы системы;
- возможность связи и операционной совместимости с национальными или международными сетями и совместимость модальностей;
- сбалансированность ключевых эксплуатационных требований любой биометрической системы, используемой для целей борьбы с терроризмом, с точки зрения безопасности, доступности для клиентов и удобства использования, пропускной способности и скорости обработки данных.

Справочные материалы к разделу 5

Резолюции 1373(2001), 1624 (2005), 2178 (2014), 2195 (2014) и 2396 (2017) Совета Безопасности ООН и резолюции A/RES/68/276 и A/70/L.55 Генеральной Ассамблеи ООН

Публикация Агентства ЕС по основным правам 'Under Watchful Eyes — Biometrics, EU-IT Systems & Fundamental Rights http://fra.europa.eu/en/publication/2018/biometrics-rights-protection

S/2015/975, пункт 8; S/2015/939, принцип 15 (e)

Резолюция A/HRC/RES/34/7 (2017) Совета по правам человека

Комитет по правам человека, замечание общего порядка № 16: Статья 17 (Право на неприкосновенность частной жизни), пункты 3 и 4

Доклад Специального докладчика по вопросу о праве на неприкосновенность частной жизни, A/HRC/31/64 (2016)

Всеобщая декларация прав человека и МПГПП, преамбула. МПГПП, статьи 2 (1), 2 (3), 9, 14 и 26

Комитет по правам человека, замечание общего порядка № 16 (1988), см.: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en

Резолюция 45/95 (1990) Генеральной Ассамблеи о руководящих принципах регламентации компьютеризованных картотек, содержащих данные личного характера, и Общий регламент Европейского союза по защите данных, 2018 год, статья 51 (Надзорный орган)

Доклад Специального докладчика по вопросу о праве на неприкосновенность частной жизни, A/HRC/31/64 (2016)

Всеобщая декларация прав человека, преамбула

Перечень инструментов по борьбе с отмыванием денег и иными формами мошенничества, приводимый на веб-сайте Международного валютного фонда www.imf.org

Международная организация по стандартизации http://www.iso.org

Международная электротехническая комиссия http://www.iec.ch

Европейский комитет по стандартизации https://www.cen.eu

Национальный институт стандартов и технологий (США) http://www.nist.gov

Общий регламент Европейского союза по защите данных, 2018 год, статья 7 (Согласие), статья 17 (Право на уничтожение данных), статья 15 (Право на доступ к данным)

Статья 19 Международного пакта о гражданских и политических правах, касающаяся права на свободное выражение мнения

УВКБ ООН, «Решение проблем безопасности без отрицательных последствий для защиты беженцев» http://www.refworld.org/docid/5672aed34.html

Декларация прав человека Организации Объединенных Наций, статья 9 (свобода от произвольного ареста и изгнания) и статья 11 (право считаться невиновным до тех пор, пока виновность не будет установлена)

Заявление по итогам встречи министров иностранных дел, состоявшейся в Мадриде 28 июля 2015 года в связи с проведением специального совещания Контртеррористического комитета Совета Безопасности

Британская группа по этическим аспектам биометрии и криминалистики http://www.gov.uk/government/publications/biometrics-and-forensics-etchics-group

Руководство Института биометрии по вопросам неприкосновенности биометрических данных, разработанное для международного использования (Biometrics Institute's Biometric Privacy Guidelines designed for international use) www.biometricsinstitute.org

Стандарт ИСО/МЭК 30107-2_2017. Обнаружение атаки на биометрическое представление. Форматы данных

[2] Frontex, Vulnerability Assessment and Testing for Automated Border Control (Abc) Systems (2017)

[3] Ted Dunstone and Neil Yager, Biometric System and Data Analysis: Design, Evalua-tion and Data Mining (2008) Springer

Стандарты ИСО/МЭК 27001:2013. Информационные технологии — Техники безопасности — Системы менеджмента информационной безопасности — Требования

Стандарт ИСО 31000:2009. Менеджмент риска — принципы и руководство

Стандарт МЭК 31010:2009. Менеджмент риска. Методы оценки риска

NIST SP 800-30 Guide for Conducting Risk Assessments

NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach

Стандарт ИСО/МЭК 17025:2017. Общие требования к компетентности испытательных и калибровочных лабораторий

6. Биометрические системы и базы данных, используемые для борьбы с терроризмом

В разделе 6 содержится общий обзор используемых для борьбы с терроризмом биометрических систем и баз данных, имеющих широкий спектр применения в правоохранительной деятельности, в деятельности по управлению границами в военной сфере. В нем также рассмотрены выгоды от обмена биометрическими данными на двусторонней и многосторонней основе, в региональных и глобальных масштабах и показано, как биометрические данные в сочетании с другими оперативными данными можно использовать не только в традиционном качестве следственного инструмента, но и для предупреждения террористических актов. Затем меры, принимаемые властями в случае совпадения биометрических данных, рассматриваются в контексте международных стандартов прав человека и необходимости принятия ответных мер на принципах полной информированности, законности и соразмерности. В заключительной части раздела речь идет о включении биометрических данных в стратегии борьбы с терроризмом, применяемые государствами-членами и регионами, а также о важной роли пограничных служб и правоохранительных органов в активной поддержке таких стратегий.

6.1. Современные биометрические системы и базы данных, используемые для борьбы с терроризмом

6.1.2. Приложения, применяемые пограничными службами

Все более совершенствующиеся процедуры пограничного контроля[49] играют важнейшую роль в борьбе с терроризмом в целом и в перехвате иностранных боевиков-террористов в частности. Особенности и масштаб работы пунктов пересечения границы (ППГ) во многом зависят от вида транспорта. В сфере международного воздушного сообщения ППГ в значительной степени унифицированы. Что касается наземного, водного и морского сообщения, то в этой сфере, как правило, существует два вида ППГ: один предназначен для всех лиц, совершающих международные поездки, а другой — для въезда и выезда граждан данной страны. Лица, совершающие международные поездки, обязаны пройти через ППГ, чтобы въехать на территорию страны на законных основаниях. ППГ для местного населения обычно располагаются на сухопутных границах или в назначенных портах, обслуживающих два или несколько сопредельных государств. Эти местные ППГ часто создаются в рамках экономических зон (представляющих собой 25-километровые полосы по обе стороны государственной границы), открытых для граждан обоих сопредельных государств. Прочие лица, совершающие международные поездки, пользоваться этими местными ППГ не могут.

ППГ на международных границах фактически играют роль эффективного фильтра, в котором критерии отбора можно ужесточить или смягчить в зависимости от уровня угрозы. Как правило, этот фильтр находится на «нормальном» уровне, но при усилении угрозы контроль может быть ужесточен до «оранжевого» или даже «красного» (или аналогичных) уровней, а в некоторых чрезвычайных ситуациях граница закрывается полностью. В ситуациях, когда для большого числа людей может возникнуть необходимость быстрого въезда в страну, например в случае стихийного бедствия или антропогенной катастрофы в соседней стране, граница может быть открыта для обеспечения беспрепятственного доступа, а необходимые официальные проверки будут проведены позднее, как только люди перейдут границу и окажутся в безопасных зонах.

Пограничный контроль пассажиров и товаров осуществляется иммиграционными службами, контрольно-пропускными службами и службами безопасности, охраны правопорядка, таможни и карантина. Пограничным службам необходимо создать условия для эффективной оперативной деятельности, включая комплектование подготовленным и мотивированным персоналом, обеспечение высокотехнологичным оборудованием и регулярно обновляемой информацией. Важным компонентом

[49] «Термин "пограничная линия" обычно используется в качестве обозначения линии, разделяющей территории или морское пространство двух государств, в то время как "граница" — это то, что пересекают, чтобы попасть на территорию государства. Иногда граница и пограничная линия полностью совпадают, но чаще понятие "граница" включает определенную инфраструктуру — пункты иммиграционного контроля, таможенные посты, ограждения и патрульные дороги, выходящие за пределы пограничной линии; в международных аэропортах и морских портах граница может располагаться на расстоянии в сотни километров от пограничной линии. Пограничная линия, по сути, является некоей определенной линией, в то время как граница, как правило, представляет собой более сложную структуру, состоящую из нескольких линий и/или зон, предназначенных в первую очередь для регулирования перемещения людей и грузов». *Мартин Пратт, профессор Даремского университета, Соединенное Королевство*.

современных ППГ являются биометрические приложения, значительно упрощающие процедуры пограничного контроля. Они являются составной частью более широкой технологической системы, охватывающей все аспекты международных поездок — с момента организации поездки до прибытия и окончательного выезда совершающего поездку лица из страны. Информация о всех этапах этого процесса поступает из различных источников, сводится воедино и предоставляется сотруднику службы пограничного контроля, который использует ее вместе с другой информацией для принятия решения относительно допуска совершающего поездку лица на территорию страны.

Наиболее развитой в этом отношении сферой является международное воздушное сообщение, и именно оно в прошлом стимулировало развитие основанных на стандартах технических инноваций, которые впоследствии применялись на сухопутных и морских границах. Скорее всего, по этой же традиционной модели пойдет и развитие формирующейся сейчас практики применения биометрии для идентификации террористов. Современная система пограничного контроля, применяемая в сфере международного воздушного сообщения, позволяет повторять процедуру идентификации пассажира и оценку рисков в процессе перемещения пассажира по мере получения дополнительной информации государством назначения или выезда. Основными источниками данных о пассажирах в сфере международного воздушного сообщения являются авиационные компании и правительства, и именно эти источники данных используются в новых разработках биометрических систем.

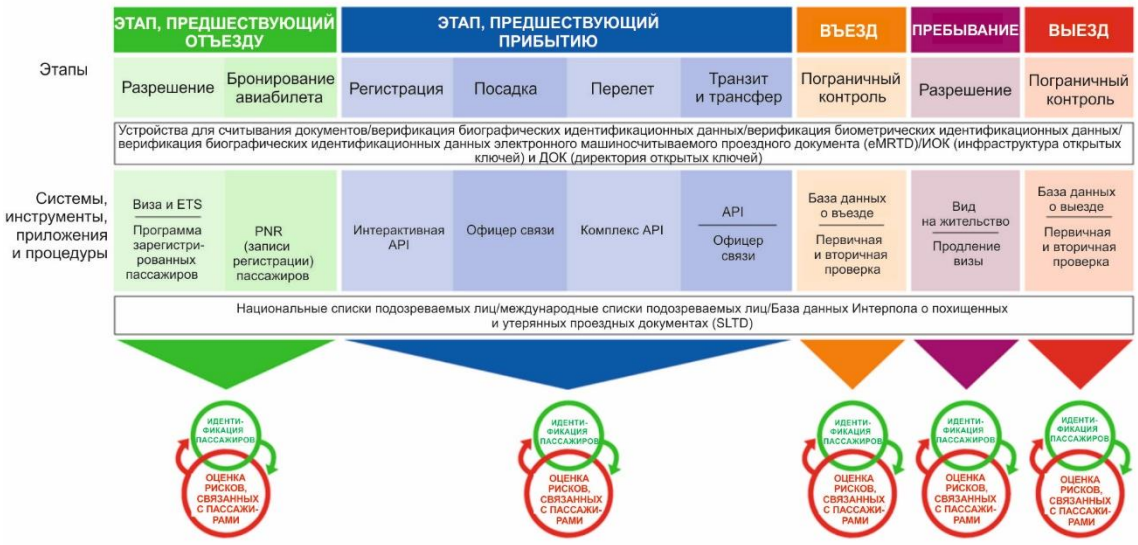


Рисунок 4. Пять этапов цикла поездки[50]
(с разрешения ИКАО)

С точки зрения государств назначения процесс поездки от начала до конца делится на пять этапов (см. рисунок 4):

1) этап, предшествующий отъезду;
2) этап, предшествующий прибытию;
3) въезд;
4) пребывание;
5) выезд.

При этом с точки зрения системы в целом и в международном плане поездка представляет собой цикл, поскольку процесс обработки данных для выезда из государства, в котором начинается поездка, в то же время является процессом обработки данных на этапе, предшествующем прибытию, с точки зрения соответствующих государств транзита и назначения.

[50] Более подробную информацию см. в ICAO TRIP Guide on Border Control Management, Montreal (2018).

Этап 1. Этап, предшествующий отъезду

В настоящее время многие государства требуют от всех лиц, совершающих поездку, представить предварительную информацию еще до их прибытия на границу. Эта информация включает главным образом биографические сведения, документы и данные о поездке. Кроме того, государства все чаще требуют представления биометрической информации для подтверждения идентичности въезжающих граждан иностранных государств. В прошлом лица, совершающие поездку, делились на две группы: те, кому нужна была виза для въезда в страну, и те, кому виза была не нужна. Начиная с 1990-х годов государствам доступны данные из систем контроля отправки пассажиров авиакомпаний в виде предварительной информации о пассажирах (API) и интерактивной API. В настоящее время государства собирают предварительную информацию о пассажирах до начала поездки, используя ряд различных механизмов. На сегодняшний момент для сбора информации перед прибытием пассажира в страну используются следующие процедуры и системы.

1.a. Подача «классического» заявления на получение визы. Общее для многих стран требование, основанное на исторических, дипломатических и экономических факторах, а также на политических отношениях государства с другими странами. Эта процедура обычно предусматривает предоставление заявителем биографических и биометрических идентификационных признаков в рамках комплексного процесса подачи заявления, включающего также представление проездных документов и уплату сбора дипломатическому учреждению или представителю страны назначения. Биометрические данные могут быть представлены в виде фотографии лица или регистрационных данных, например отпечатков пальцев. За этим следует проверка заявления, заявителю виза либо будет выдана, либо он получит отказ в ее выдаче. Проверка данных до выдачи визы может включать поиск по модели 1:n в списках биометрических данных подозреваемых лиц, если соответствующие государства сформировали массивы данных для этой цели.

1.b. Подача заявления на получение региональной визы. Региональное сотрудничество между странами широко распространено, и на каждом континенте существует как минимум одна региональная организация: например, АСЕАН[51] в Юго-Восточной Азии, ЭКОВАС[52] в Западной Африке, ЕС в Европе, УНАСУР[53] в Южной Америке, КАРИКОМ[54] в Карибском бассейне. Уровень сотрудничества в рамках этих объединений неодинаков. Примером такой региональной системы служит Европейский союз, где был принят регламент, обязывающий каждое входящее в ЕС государство создать свою собственную визовую информационную систему (ВИС). Эти системы присоединены к центральному узлу ВИС, который регулируется Европейским агентством по оперативному управлению масштабными ИТ-системами (eu-LISA). ВИС проводит проверку биометрических данных — фотографии лица и набора из десяти отпечатков пальцев — для верификации идентичности пассажира на границе, а также проверку биографических данных по второй версии Шенгенской информационной системы (ШИС II)[55] и национальным базам данных. Архитектура этих региональных систем позволяет проводить до выдачи визы проверку данных, включающую поиск по модели 1:n в списках биометрических данных подозреваемых лиц, если соответствующие государства и регионы сформировали массивы данных для этой цели.

1.c. Подача заявления на получение визы через сторонние организации. В данной модели, приобретающей все бóльшую популярность во многих странах, действующие на коммерческих началах поставщики услуг собирают и комплектуют все документы и данные заявителя, необходимые для подачи заявления на получение визы. При этом может быть предусмотрена регистрация биометрических данных заявителя (изображения лица, сканов радужной оболочки глаза и/или отпечатков пальцев). Затем заявление на получение визы направляется соответствующему дипломатическому представительству для

---

51 АСЕАН — Ассоциация государств Юго-Восточной Азии.

52 ЭКОВАС — Экономическое сообщество западноафриканских государств.

53 УНАСУР — Союз южноамериканских наций.

54 КАРИКОМ — Карибское сообщество.

55 Государства — участники Шенгенского соглашения используют ШИС II Европейского союза в рамках сотрудничества по вопросам общественной безопасности, пограничного контроля и правоприменения в Европе. Государства обмениваются информацией, полученной из полицейских баз данных и списков подозреваемых лиц, составленных службами пограничного контроля. Доступ к этой информации можно получить как внутри страны, так и на границах; кроме того, эту информацию используют для проверки лиц, въезжающих в Европейский союз и выезжающих из него. В системе содержатся данные о разыскиваемых и пропавших лицах, утерянных или похищенных идентификационных/проездных документах, биометрические данные, информация об угнанных автомобилях и т.д.

проведения необходимых проверок и принятия решения о выдаче визы. Проверка данных до выдачи визы может включать передачу государству биометрического изображения или шаблона для проведения поиска по модели 1:n в списках биометрических данных подозреваемых лиц, если такое государство сформировало массив данных для этой цели.

1.d. Подача заявления на получение визы в онлайновом режиме или на получение электронной визы. Процедура подачи заявления на получение визы осуществляется полностью в онлайновом режиме с использованием электронных форм и сканированных изображений фотографии заявителя (в соответствии с требованиями ИКАО) и страницы паспорта с биографическими данными. Процедуры принятия решения и проведения любых проверок биометрических данных осуществляются централизованным образом. В случае выдачи визы заявитель получает соответствующее подтверждение, а на границе проводится верификация его биометрических данных по модели 1:1, т.е. лицо заявителя сопоставляется с представленной фотографией для подтверждения того, что заявитель и пассажир — одно и то же лицо. Проверка данных до выдачи визы может включать проведение поиска по модели 1:n в списках биометрических данных подозреваемых лиц, если соответствующие государства сформировали комплексы данных для этой цели.

1.e. Электронные системы авторизации поездок (ETS). В рамках данной процедуры производится сбор базовых идентификационных данных пассажиров независимо от визовых требований. Эта процедура аналогична подаче заявления на получение визы в онлайновом режиме или электронной визы, но сбор биометрических данных, кроме фотографии лица, производится на границе, а не на этапе перед отъездом.

Другим важным источником данных, собираемых до начала поездки, являются авиакомпании[56].

1.f. Система учетных записей пассажира (PNR). После получения пассажиром визы или разрешения на поездку следующим этапом является бронирование авиабилета путем внесения данных PNR в онлайновом режиме. Авиакомпания хранит данные PNR в компьютерной системе бронирования (КСБ) и использует их в коммерческих и операционных целях, но также предоставляет их органам пограничного контроля перед выездом пассажира. ВТамО совместно с ИАТА и ИКАО разработала и ввела в действие технические стандарты (PNRGOV)[57] для согласованного обмена данными PNR между авиаперевозчиками и правительствами. *В записях PNR не содержатся биометрические данные.* Ценность данных PNR заключается в том, что они содержат важную контекстную информацию, способствующую повышению эффективности идентификации и целенаправленному выявлению пассажиров, внушающих обеспокоенность, на основании имеющихся рисков.

Этап 2. Этап, предшествующий прибытию

2.a. Сбор *предварительной информации о пассажирах (API)* осуществляется системами контроля отправлений авиаперевозчика. Сбор API осуществляется постепенно на этапе регистрации, однако передача этой информации государственным органам страны назначения происходит только после регистрации всех пассажиров, их посадки и закрытия дверей воздушного судна. Важно отметить, что дополнительный сбор API осуществляется на транзитных остановках дальнемагистральных авиарейсов. При сборе API используются два источника данных: 1) информация из машиносчитываемой зоны паспорта пассажира и 2) подробные сведения о авиарейсе и информация о регистрации, которые могут включать как стандартные, так и дополнительные элементы данных, в том числе сведения о зарегистрированном багаже, номерах мест, количестве пассажиров на борту, номере рейса, дате, времени и месте отправления и прибытия. Это позволяет органу пограничного контроля государства назначения провести предварительную проверку пассажиров до их прибытия. Принятый в настоящее время стандарт передачи данных API *не предусматривает передачи биометрических данных, однако в будущем может появиться возможность сбора фотографий, соответствующих требованиям ИКАО, из бесконтактного чипа паспорта/проездного документа. Для этого потребуется установка на стойках регистрации или в терминалах регистрации устройств для считывания электронных паспортов, однако на сегодняшний момент не все страны располагают этой технологией.*

---

[56] Стандарты и рекомендуемая практика касательно PNR и API приводятся в главе 9 «Система обмена данными о пассажирах» 15-го издания приложения 9 к Чикагской конвенции. ВТамО, ИАТА и ИКАО совместно разработали и согласовали стандарты электронных сообщений, включающих массивы данных, в Рекомендациях в отношении PNR (Doc 9944) и API.

[57] PNRGOV EDIFACT & XML Message Implementation Guide: www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx.

2.b. Интерактивная предварительная информация о пассажирах (iAPI). Это усовершенствованная версия API, передающая информацию о пассажире надлежащему органу пограничного контроля в момент электронной регистрации. Информация о каждом пассажире передается отдельно, а не в пакете, как в процессе передачи API. Процедура iAPI позволяет осуществлять проверку списка подозреваемых лиц и другие проверки до того, как пассажир попадет на борт воздушного судна; таким образом, эта процедура создает дополнительный уровень защиты воздушного судна, пассажиров и страны назначения. *Обращение с биометрическими элементами при проведении данной процедуре аналогично обращению с биометрическими элементами при процедуре сбора API, описанному выше в пункте 2a.*

Пример из практики 5. Въезд без предъявления проездного документа

В настоящее время рассматривается возможность использования автоматизированной системы пограничного контроля (АСПК) следующего поколения для поездок, совершаемых между Австралией и Новой Зеландией. АСПК повысит эффективность существующих систем сбора iAPI, поскольку сможет осуществлять сбор изображений лиц из паспортных и визовых баз данных для создания динамичной базы данных об ожидаемых прибытиях для каждого прибывающего авиапассажира. При использовании данного приложения пассажиру не нужно вынимать электронный паспорт из кармана: биометрическая АСПК сравнивает изображение лица пассажира с изображением из базы данных об ожидаемых прибытиях и разрешает въезд на территорию страны только при условии совпадения этих изображений. Разрабатываемое приложение пригодно для маломасштабной биометрической идентификации 1:n.

В дополнение к проверке на предшествующем прибытию этапе ряд государств привлекают офицеров связи — государственных служащих стран назначения — к работе в аэропортах посадки и транзита для оказания авиакомпаниям помощи в идентификации пассажиров и оценке рисков.

Этап 3. Въезд

Пассажир может начать поездку только после успешного завершения всех процедур на этапе, предшествующем прибытию. Тем не менее для большинства стран завершение процедур этапа 1 (предшествующего отъезду) и этапа 2 (предшествующего прибытию) еще не гарантирует пассажиру въезда в страну назначения. Окончательное решение принимает сотрудник службы пограничного контроля, которому пассажир по прибытии представляет необходимые документы и идентификационные данные. Сотрудник иммиграционной службы должен принимать решение, опираясь на целый ряд факторов, и для упрощения этой процедуры были разработаны информационные системы пограничного контроля (ИСПК). Тем не менее следует отметить, что некоторые международные ППГ до сих пор не имеют доступа к технологии ИСПК. ИСПК существенно различаются с точки зрения технологического уровня их функциональных возможностей. В более технологически продвинутых странах все шире практикуется верификация на основе биометрических идентификационных данных. Гораздо менее распространено использование списков биометрических данных подозреваемых лиц. Существуют следующие основные варианты ИСПК.

3.a. Стандартная информационная система пограничного контроля (ИСПК). Национальное право и законодательство регулируют количество и характер осуществляемых на границе проверок, например определяют, следует ли регистрировать подробные данные всех лиц, въезжающих на территорию страны, или только проводить поиск в списках подозреваемых лиц или санкционных списках. Странам, регистрирующим данные всех лиц, въезжающих на их территорию, необходим тот или иной вид ИСПК. Регистрация данных может осуществляться вручную, но в большинстве современных систем применяется устройство для считывания паспорта, выгружающее данные из машиносчитываемой зоны проездного документа, а сотрудник службы пограничного контроля осуществляет ввод дополнительной информации, касающейся идентификационных данных, продолжительности и причины посещения, адреса проживания в стране и т.д. Затем проводится поиск данных в списках подозреваемых лиц. *Стандартная ИСПК не осуществляет сбор биометрических данных для автоматизированной верификации.*

3.b. Электронная информационная система пограничного контроля (э-ИСПК). В э-ИСПК используется электронное устройство для считывания паспорта, предоставляющее доступ к бесконтактному чипу в электронном машиносчитываемом проездном документе (эМСПД)[58]. В чипе

[58] eМСПД — МСПД (паспорт или идентификационная карта) со встроенной в него бесконтактной интегральной схемой, который можно использовать для биометрической идентификации владельца данного МСПД в соответствии со стандартами, изложенными в соответствующей части Doc 9303 ИКАО — «Машиносчитываемые проездные документы».

содержатся данные машиносчитываемой зоны (МСЗ) и цифровая фотография лица, соответствующая требованиям ИКАО, а зачастую — еще и два отпечатка пальцев. В некоторых странах доступ к этим отпечаткам пальцев для целей верификации предоставляется только в том случае, если э-ИСПК имеет цифровой сертификат, предоставленный страной выдачи визы и разрешающий открытие группы данных, содержащей отпечатки пальцев. Для верификации личности на основе биометрических данных, содержащихся в чипе, э-ИСПК должна быть соединена с биометрической системой и иметь возможность осуществлять сбор биометрических данных пассажиров при помощи камеры — для получения изображения лица, инфракрасной камеры — для получения снимка радужной оболочки глаза, а также считывающего устройства для отпечатков пальцев, с тем чтобы сравнить полученные данные с данными, содержащимися в чипе. Электронная ИСПК поддерживает проведение верификации биометрических идентификационных данных 1:1 при помощи изображений биометрических признаков, считанных из электронного паспорта. Электронная ИСПК также может осуществлять поиск 1:n в списках биометрических данных подозреваемых лиц, если соответствующие государства сформировали массивы данных для этой цели.

Чтобы не быть обнаруженными при пересечении границы, террористы могут использовать поддельные проездные документы. Они применяют различные приемы — от подмены фотографии или использования паспорта человека с похожей внешностью до создания поддельной копии всего документа. Поэтому автономное устройство для считывания электронных паспортов, присоединенное к комплексной биометрической системе, является ценным инструментом проверки документов, используемым в борьбе с подделкой паспортов, особенно на ППГ с ограниченными ресурсами для борьбы с мошенничеством такого рода. Размещение подобного оборудования в местах вторичной проверки может значительно упростить работу сотрудников служб пограничного контроля при проверке пассажиров, чьи документы впервые вызвали подозрения на ППГ.

Пример из практики 6. Логическая структура данных, версия 2

Новой разработкой, которая может упростить доступ к дополнительным биометрическим данным, хранящимся в электронных паспортах, является логическая структура данных (LDS), версия 2. LDS хранится в бесконтактном чипе электронного паспорта или проездного документа, ее можно сравнить со «шкафом» с 16 «ящиками», которые называются группами данных. Часть хранящейся информации является обязательной, другую, дополнительную, часть страны могут добавлять по своему усмотрению. Группы данных должны соответствовать требованиям структуры ИОК ИКАО[59]. Это является гарантией того, что данные, содержащиеся в LDS, были предоставлены учреждением, обладающим соответствующими полномочиями, не подвергались изменениям или не были аннулированы. В версии LDS-2 к структуре LDS добавлены еще три компонента, а именно: 1) данные о поездке, отметки о въезде и выезде, 2) данные о визе и 3) дополнительные биометрические данные. По усмотрению органа, занимающегося выпуском электронных паспортов, LDS-2 может быть сохранена в бесконтактном чипе электронного паспорта при выпуске новых электронных паспортов.

Это значит, что визовые службы и службы пограничного контроля отныне могут записывать информацию, касающуюся трех новых групп данных, на бесконтактные чипы другой страны. Служба пограничного контроля может сохранять данные о поездке, проставляя в паспорте электронную отметку, соответствующие органы могут вносить данные о визе непосредственно в группу данных, а электронная проверка может быть осуществлена непосредственно по прибытии на границу. Соответствующие биометрические шаблоны пассажиров, участвующих в программах зарегистрированных пассажиров, могут храниться в их электронных паспортах и применяться для прохода пассажиров через терминалы АСПК в странах — участницах программы.

Примечание. Обязательным правовым условием для добавления новых данных на бесконтактный чип является обмен сертификатами ИОК ИКАО между органом, занимающимся выпуском электронных паспортов, и страной, выражающей желание записать эти данные. LDS-2 можно использовать только при выполнении этого правового условия.

[59] ИОК (инфраструктура открытых ключей) — согласно определению ИКАО, набор мер политики, процедур и технологий, используемых для верификации, регистрации и сертификации пользователей приложения по обеспечению безопасности. В ИОК применяются принципы криптосистемы с открытым ключом и сертификации ключей в целях обеспечения безопасной связи.

3.c. Электронная информационная система пограничного и биометрического контроля (э-ИСПБК). Эта система аналогична системе э-ИСПК, за исключением использования считывающего устройства для электронных паспортов, поскольку регистрация биометрических данных осуществляется на границе и через визовую систему. Преимущество этой системы заключается в том, что всю процедуру обработки биометрических данных выполняет страна назначения, и, таким образом, должностные лица получают возможность контролировать качество регистрации и добиваться максимально эффективной работы системы биометрической верификации по модели 1:1. Например, благодаря принятию этой архитектуры Соединенные Штаты получили возможность проводить сопоставление по модели 1:n списков биометрических данных подозреваемых лиц с обширными списками подозреваемых лиц, составленных правительством США, в отношении всех прибывающих в страну лиц с иностранными паспортами.

3.d. Автоматизированная система пограничного контроля (АСПК). В последние десятилетия стремительный рост численности лиц, совершающих международные поездки, стимулирует внедрение технических новшеств и автоматизации в пограничной инфраструктуре. Первая автоматизированная система пограничного контроля была внедрена в аэропорту Схипхол в Нидерландах; с тех пор АСПК распространились по всему миру и в настоящее время используются на постоянной основе во многих странах. В современных вариантах этой системы применяются быстродействующие датчики и биометрические данные, хранящиеся в чипе электронных проездных документов, такие как лицо, радужная оболочка глаза и отпечатки пальцев, с помощью которых проводится биометрическая верификация по модели 1:1, обеспечивающая автоматический проход через пограничные пункты. Это позволяет обеспечить быстрый проход через ППГ с минимальными задержками для большого числа граждан предварительно оговоренных стран или представителям приоритетных групп пассажиров, а сотрудникам служб пограничного контроля — сосредоточиться на других пассажирах, в отношении которых может понадобиться более тщательная проверка. Руководствуясь текущими оценками риска и соответствующим законодательством, национальные или региональные органы власти вправе в любой момент принять решение о том, граждане каких стран или представители каких групп могут проходить через терминалы АСПК. Системы АСПК могут вести поиск по модели 1:n в списках биометрических данных подозреваемых лиц, если соответствующие государства сформировали массивы данных для этой цели.

Этап 4. Пребывание

Каждая страна обязана осуществлять контроль над лицами, не являющимися гражданами этой страны и въезжающими на ее территорию на короткий или на более длительный срок, либо постоянно проживающими в этой стране. Эта задача может быть возложена на различные органы власти и учреждения, в зависимости от нормативно-правовой базы данной страны, однако их функции будут одинаковыми — например, выдача видов на жительство и студенческих виз, рассмотрение ходатайств о предоставлении статуса беженца, о предоставлении убежища и о натурализации, а также осуществление правоприменительных функций, например решение вопросов, касающихся превышения иностранцами срока законного пребывания в стране, расследование преступлений, связанных с торговлей людьми и эксплуатацией труда, и т.д.

Наглядным примером подобных региональных систем являются европейские системы ВИС и ШИС II, действующие в Европейском союзе и описанные выше в разделе «Этап 1.b». При помощи этих баз данных все соответствующие органы власти в странах ЕС могут вести учет иностранных граждан на своих территориях. Кроме того, следует отметить систему Eurodac — централизованную базу данных ЕС, осуществляющую сбор и обработку цифровых отпечатков пальцев лиц, ходатайствующих о получении убежища. В настоящее время этой базой данных пользуются 28 стран ЕС, а также Норвегия, Исландия, Швейцария и Лихтенштейн. Система Eurodac осуществляет обработку, хранение и/или сопоставление отпечатков пальцев граждан третьих стран или лиц без гражданства в возрасте 14 лет и старше, 1) подавших ходатайство о получении убежища в одной из стран — участниц системы Eurodac, или 2) задержанных в связи с несанкционированным пересечением внешних границ, или 3) незаконно пребывающих на территории одной из стран — участниц системы Eurodac. Кроме того, Eurodac играет важную роль в осуществлении Дублинского регламента. Этот документ регламентирует подачу ходатайств о получении убежища и призван предотвращать подачу одним и тем же лицом нескольких ходатайств о получении убежища в разных странах ЕС. Основной целью регламента является возложение ответственности за дальнейшую обработку ходатайства о получении убежища на одно государство-член, чаще всего на страну первого въезда в ЕС лица, подающего ходатайство. С июля 2015 года правоохранительным органам предоставляется ограниченный доступ к базе данных Eurodac, при соблюдении очень строгих условий, для целенаправленного поиска отпечатков пальцев. Поиск должен

проводиться в индивидуальном порядке и только в целях предотвращения, выявления и расследования определенных серьезных преступлений и террористических актов.

Биометрические данные, собранные органами пограничного контроля на ранних этапах поездки, могут быть предоставлены правоохранительным органам и службам безопасности в рамках сбора соответствующих следственных или оперативных данных.

Этап 5. Выезд

Процедуры, осуществляемые на этапе, предшествующем выезду, аналогичны процедурам на этапе, предшествующем въезду. Пассажир должен пройти электронную регистрацию или регистрацию в аэропорту и представить свои документы перед посадкой на рейс. АСПК дополняются целым рядом программ для часто путешествующих пассажиров, например такими, как «программа зарегистрированных пассажиров». Пассажиры, участвующие в таких программах, должны зарегистрироваться для получения членства и представить биометрические данные, а участники некоторых программ также должны пройти процедуру проверки. Например, в США действует программа Global Entry, позволяющая заранее одобренными пассажирам с низким уровнем риска проходить ускоренную проверку при пересечении границ США. Участники программы проходят к специальным терминалам Global Entry, представляют свой машиносчитываемый паспорт или постоянный вид на жительство в США, прикасаются пальцами к датчику для проверки отпечатков пальцев и заполняют таможенную декларацию. Терминал выдает пассажиру квитанцию о прохождении проверки. Пассажиры должны быть заранее одобрены для участия в программе Global Entry. Все подающие заявление о присоединении к программе должны до регистрации пройти тщательную проверку и очное собеседование.

Хотя не все страны осуществляют паспортный контроль на этапе выезда пассажира из страны, однако многие все же проводят проверку пассажира, покидающего их территорию. Как правило, в таких случаях органы пограничного контроля проверяют, совпадает ли имя на посадочном талоне с именем в проездном документе, проводят поиск этого имени в списках биографических данных подозреваемых лиц, выясняют, соответствуют ли данные авиарейса расписанию на текущий день и не превысил ли пассажир срок пребывания в стране. Кроме того, при проверке пассажиров осуществляется поиск курьеров, перевозящих наркотики и денежные средства, лиц, незаконно вывозимых в другие страны, и в особенности — иностранных боевиков-террористов. Поиск производится на основе проездных документов, посадочных талонов и других конкретных критериев.

Пример из практики 7. Биометрическая верификация при выезде

Новая модель, формирующаяся в настоящее время в Соединенных Штатах, предполагает партнерское сотрудничество авиакомпаний, аэропортов и государства в целях инвестирования средств в инициативы по упрощению процедур выхода на посадку, обеспечивающие альтернативный механизм биометрической верификации при выезде. В начале 2018 года авиакомпании «Люфтганза» и «Бритиш эйруэйз» провели испытания системы идентификации по лицу. Это еще один вариант применения биометрической верификации *1:n* известных путешественников, аналогичный механизмам, которые разрабатываются в рамках партнерства между авиакомпаниями и государством для полетов между Австралией и Новой Зеландией (см. пример из практики 5).

6.1.3. Приложения, применяемые органами полиции и Интерполом

Базы биометрических данных, используемые органами полиции (см. разделы 4.3 и 4.4), обычно содержат эталонные данные арестованных лиц (изображения лиц, отпечатки пальцев и профили ДНК), данные с места преступления и иные неидентифицированные данные, например сведения из запросов о пропавших или умерших лицах, либо данные, полученные в ходе оперативной деятельности. Эти системы могут действовать на местном, региональном или национальном уровнях и использоваться для выполнения таких функций, как ведение криминалистического учета, расследование преступлений или анализ оперативных данных судебной экспертизы. Биометрические данные, полученные при расследовании дел о терроризме, можно либо добавлять в эти системы, либо загружать в специальные базы данных в качестве дополнительной меры обеспечения безопасности. Независимо от используемой конфигурации базы данных может возникнуть оперативная необходимость проведения поиска по всем системам из-за потенциально возможных пересечений между терроризмом и общей преступностью, когда, например, уголовные преступники совершают мошенничество или хищение ценностей специально

для финансирования террористической деятельности и т.д. *В идеале эти системы также должны быть совместимы с биометрическими приложениями, используемыми пограничными службами, если это разрешено национальным законодательством.*

На международном уровне полиция может осуществлять обмен биометрическими данными в рамках двусторонних, многосторонних или региональных соглашений, однако единственным официальным глобальным методом является обмен данными через Международную организацию уголовной полиции (МОУП, более известную как Интерпол), которая содействует международному полицейскому сотрудничеству. Следует заметить, что страны, предоставляющие данные в базы данных Интерпола:

1) *сохраняют право собственности на свои данные* и в любой момент могут удалить их из баз данных (см. раздел 6.3 «Односторонний поиск»);
2) *определяют объем данных, по которым осуществляется поиск*, т.е. их данные, по которым осуществляется поиск, и картотечные данные не предоставляются для сопоставления с биометрическими данными из определенных стран.

Интерпол располагает тремя базами биометрических данных, которыми могут пользоваться все его 190 стран-членов.

Изображения лиц — обеспечивает следующие функциональные возможности:

- идентификация лиц, скрывающихся от правосудия, и пропавших без вести;
- идентификация неизвестных лиц, представляющих интерес;
- идентификация лиц на изображениях в СМИ;
- верификация сделанных в полиции фотографий (снимков взятых под стражу) по базе данных (1:n).

Отпечатки пальцев — шлюз AFIS. Эта система предоставляет уполномоченным сотрудникам правоохранительных органов из стран-членов возможность удаленного доступа к базам данных и получения автоматического ответа с использованием защищенной глобальной телекоммуникационной сети Интерпола I-24/7. База данных содержит как эталонные данные (отпечатки пальцев и ладоней), так и данные с места преступления (следы пальцев и ладоней).

ДНК — шлюз ДНК (который действует аналогично шлюзу AFIS). Интерпол согласовал правила обработки данных ДНК со всеми странами-членами, и соответствующая база данных состоит из четырех разделов:

- места нераскрытых преступлений;
- известные полиции правонарушители;
- лица, пропавшие без вести;
- неопознанные человеческие останки.

Интерпол также предлагает услуги, предоставляемые устройством двустороннего сопоставления ДНК в качестве частной платформы для поиска и сравнения ДНК и обмена этими данными между двумя странами. Основу этого механизма составляют взаимное доверие, полицейская стратегия, совместимое законодательство и взаимосогласованные критерии сопоставления, например минимальное количество локусов. Каждая страна отбирает профили ДНК и отправляет их в Интерпол в защищенном режиме. Информация об обнаруженных совпадениях направляется обоим партнерам, после чего данные удаляются из системы. Страны могут использовать этот инструмент для разовых сравнений или в рамках регулярных операций по сопоставлению.

Важной функцией баз биометрических данных Интерпола является сбор биометрических данных иностранных террористов-боевиков и других террористов в целях предотвращения их перемещения через границы. Эта функция осуществляется в рамках того направления деятельности Глобальной контртеррористической стратегии Интерпола, которое связано преимущественно с идентификацией членов известных транснациональных террористических групп.

6.1.4. Базы биометрических данных Интерпола — надзор и управление

Надзор за внутренним управлением и функционированием баз биометрических данных Интерпола осуществляет независимый орган — Комиссия по контролю за файлами Интерпола (CCF). На нее возложены три функции:

1) обеспечение того, что порядок обработки Интерполом персональных данных соответствует регламенту этой организации;
2) предоставление Интерполу рекомендаций по любым вопросам, связанным с обработкой персональных данных;
3) обработка запросов, касающихся информации, которая содержится в базах данных Интерпола.

Статус официального органа Интерпола Комиссия получила в 2008 году, когда Генеральная Ассамблея проголосовала на своей 77-й сессии за укрепление статуса Комиссии путем внесения в Устав поправок, предусматривающих ее включение во внутреннюю правовую структуру Интерпола. В ноябре 2016 года Генеральная Ассамблея Интерпола приняла пакет реформ, касающихся надзорных механизмов Интерпола. В рамках этого пакета было принято новое Положение о Комиссии по контролю за файлами, предусматривавшее глубокое реформирование ее состава, структуры и процедур. Эти новые правовые рамки вступили в силу 11 марта 2017 года и способствовали укреплению контрольных и надзорных функций Комиссии, а также ее полномочий предоставлять гражданам эффективные средства правовой защиты в отношении касающихся их данных, которые могут обрабатываться в файлах Интерпола.

6.1.5. Управление данными биометрических и биографических списков особого внимания

Списки особого внимания — один из видов системы оповещения; они основываются на различных видах данных и действуют на национальном, а иногда на региональном уровне. Они призваны обеспечить заблаговременное оповещение и проведение процедур проверки, способствуя, таким образом, распознаванию и идентификации преступников, террористов и подозрительных товаров или материалов на пунктах пересечения границы. Существует несколько видов списков особого внимания, в том числе:

- *биографические списки особого внимания:* информация о находящихся в розыске или пропавших без вести лицах, лицах, представляющих оперативный интерес, лицах, находящихся в «черном списке» авиакомпаний, и т.д.;
- *биометрические списки особого внимания:* к наиболее распространенным модальностям относятся отпечатки пальцев, изображения лица и радужной оболочки глаза (ДНК в настоящее время широко не используется); их функционал аналогичен функционалу биографических списков особого внимания, т.е. они содержат информацию о находящихся в розыске или пропавших без вести лицах, лицах, представляющих оперативный интерес, известных террористах или лицах, подозреваемых в терроризме, и т.д.;
- *списки особого внимания, содержащие информацию о товарах и документах:* сведения об украденных транспортных средствах, утерянных и украденных проездных документах[60], украденных произведениях искусства и т.д.;
- *списки особого внимания, содержащие информацию о способах совершения преступлений или о распознавании опасных грузов:* сведения о конкретных способах совершения преступления или серии преступлений, новых способах распознавания поддельных денежных знаков или проездных документов, методах и химических компонентах, используемых для изготовления запрещенных наркотиков, и т.д.

Списки особого внимания используют международные и региональные правоохранительные органы, например Интерпол[61] и Европол[62], а также — в иных прикладных целях — организации, не имеющие отношения к охране правопорядка; таким образом, круг пользователей списков широк и разнообразен.

- *Правоохранительные органы:*

[60] См. https://www.interpol.int/INTERPOL-expertise/I-Checkit.

[61] См. https://www.interpol.int/.

[62] См. https://www.europol.europa.eu/.

- международные[63]: Интерпол[64];
- региональные: Европол[65] и иные региональные организации;
- национальные[66]: полиция, миграционные органы, таможенная служба и т.д.

- *Международные организации:*
  - Организация Объединенных Наций (ООН[67]) и т.д.
- *Государственные организации:*
  - органы, выдающие паспорта[68], органы, выдающие водительские удостоверения, и т.д.
- *Частные/коммерческие организации:*
  - авиакомпании, страховые компании, производители продуктов питания и т.д.

Организации, не имеющие отношения к охране правопорядка, используют списки особого внимания в сфере своей ответственности или хозяйственной деятельности для защиты своих изделий и процессов и предотвращения мошеннических действий.

Ограничения биографических списков особого внимания

Большинство списков особого внимания, составленных правоохранительными органами, основано на личных биографических данных, к которым относятся, например, имена, даты рождения и т.д. Эта информация может быть ненадежной, ее могут изменять или она может содержать ошибки. Вот некоторые типичные примеры:

- неправильное написание или неправильный перевод имен;
- использование измененного имени или прозвища вместо официального имени, указанного в проездных документах;
- неправильная дата рождения или неправильная последовательность цифр, например 12.01.1967 вместо 01.12.1967;
- субъект имеет двойное гражданство;
- субъект изменил свое имя и получил новое удостоверение личности или проездной документ;
- субъект предъявляет фальшивый, поддельный или полученный обманным путем проездной документ на другое имя (имена);
- субъект предъявляет подлинный проездной документ иного лица, чтобы выдать себя за настоящего владельца этого документа;
- субъект пользуется проездным документом «совместно» с кем-либо, используя «морфированную» фотографию, т.е. совмещенное изображение двух различных лиц (см. раздел 5.3.3);
- близнецы из двойни или тройни обмениваются удостоверениями личности и/или проездными документами.

Таким образом, первостепенное значение имеет положительная идентификация субъекта, что привело к созданию биометрических списков особого внимания.

Биометрические списки особого внимания

Биометрические списки особого внимания служат дополнением к процессам биометрической верификации по модели 1:1, проводимым на границе. При верификации по модели 1:1 (см. раздел 6.1.1) используются биометрические данные, хранящиеся в чипе электронного проездного документа, что позволяет аутентифицировать личность лица, прибывшего на границу. Концепция списков особого

---

63 См. ICAO TRIP Guide on Border Control Management, version 1, chapter: 5-M.

64 См. https://www.interpol.int/INTERPOL-expertise/Databases.

65 См. https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system.

66 См. ICAO TRIP Guide on Border Control Management, version 1, chapter: 4-E.

67 См. https://www.un.org/sc/ctc/.

68 См. https://www.consilium.europa.eu/prado/en/check-document-numbers/check-document-numbers.pdf.

внимания идет несколько дальше и вводит возможность поиска по модели 1:n («один-ко-многим») для проверки биометрических данных пассажира по базе биометрических данных лиц, представляющих оперативный интерес. Для обоих процессов требуется сходное оборудование для регистрации биометрических данных, однако чтобы база данных могла при необходимости выполнять обе эти функции или любую из них, потребуется программное обеспечение как для поиска по модели 1:n, так и для сопоставления по модели 1:1. Очевидно, что это потребует дополнительных инвестиций. Эффективность поиска 1:n по списку особого внимания будет зависеть от:

- качества зарегистрированных данных;
- вида данных, хранящихся в базе данных (см. раздел 4.3);
- производительности системы (см. раздел 4.1);
- степени уязвимости системы к спуфинг-атакам с использованием таких методов, как морфинг или фишинг (см. раздел 5.2).

Примерами крупных международных и региональных списков особого внимания, в частности, являются:

Интерпол I-24/7 — все базы данных Интерпола, за исключением баллистической информационной сети Интерпола (IBIN), доступны в режиме реального времени в рамках сети I-24/7, которая связывает между собой все национальные центральные бюро Интерпола (НЦБ). Она связана с системой уведомлений Интерпола, обеспечивающей распространение международных оповещений о лицах, скрывающихся от правосудия, лицах, подозреваемых в совершении преступлений, лицах, имеющих отношение к текущим уголовным расследованиям или представляющих интерес для следствия, лицах и организациях, в отношении которых введены санкции Совета Безопасности Организации Объединенных Наций, лицах, представляющих потенциальную угрозу, лицах, пропавших без вести, и трупах;

ИСЕ Европола — информационная система Европола. Эта база данных содержит криминалистическую и оперативную информацию, которая охватывает все виды преступности, относящиеся к мандату Европола, включая терроризм.

Пример из практики 8. ETIAS

Комиссия Европейского союза внесла предложение о создании Европейской информационной системы авторизации путешествий (ETIAS)[69] для укрепления безопасности поездок в Шенгенскую зону в рамках соглашений о безвизовом въезде. Список особого внимания ETIAS, который будет создан Европолом и находиться в его ведении, будет состоять из данных о лицах, подозреваемых в совершении или участии в совершении уголовного преступления, или лицах, в отношении которых имеются фактические указания или достаточные основания полагать, что они совершат уголовные преступления.

Список особого внимания будет составлен на основе:

1) списка комитета Организации Объединенных Наций по санкциям;
2) информации, относящейся к террористическим или другим серьезным уголовным преступлениям, которая предоставлена государствами-членами;
3) информации, относящейся к террористическим или другим серьезным уголовным преступлениям, которая получена в рамках международного сотрудничества.

6.2. Преимущества биометрических приложений для борьбы с терроризмом

6.2.1. В пределах государственных границ

С момента разработки первой системы классификации и поиска отпечатков в 1890-х годах роль баз биометрических данных в расследовании преступлений становится все более значимой. В XX веке компьютеризация и научно-технический прогресс существенно повысили эффективность и вычислительную мощность таких систем и расширили диапазон доступных модальностей, таких как лицо, ДНК, голос и т.д. Для биометрических поисковых систем, которые сегодня используются многими правоохранительными органами, характерно наличие усовершенствованных, сложных алгоритмов,

[69] http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282017%29583148

способных обеспечить быстрый и точный поиск в больших массивах данных. Однако основное преимущество поиска по базе данных о раскрытии и расследовании преступлений (см. раздел 4.4) по сравнению с большинством других процедур сбора следственных и оперативных данных заключается в том, что он обеспечивает круглосуточное, круглогодичное непрерывное наблюдение, которое длится до тех пор, пока данные хранятся в базе данных. Совпадение может быть найдено, как только данные оказываются зарегистрированы и начата процедура поиска, при условии что совпадающие данные уже присутствуют в базе данных; или же данные могут быть сохранены в системе, и совпадение обнаружится спустя недели, месяцы, годы или даже десятилетия. Таким образом, поиск по базе данных о раскрытии и расследовании преступлений считается одной из наиболее экономически эффективных и неизменно полезных систем, доступных современным следователям и специалистам по анализу оперативных данных. Эти базы данных также могут быть:

1) объединены на национальном уровне для обеспечения эффективного охвата страны вне зависимости от ее физических размеров и относительной населенности;
2) совместимы с биометрическими системами на пунктах пограничного контроля;
3) связаны с международными или иными соответствующими базами биометрических данных.

Криминалистическая экспертиза в режиме реального времени

Во многих странах правоохранительные органы разработали и используют эту биометрическую технологию для установления личности преступников и подтверждения их криминального прошлого, доказательства или опровержения причастности подозреваемых к совершению преступления и установления связи между преступлениями. Эти базы данных оказались особенно ценными для расследования дел о терроризме, а в последние годы их вклад стал весомее благодаря внедрению «криминалистической экспертизы в режиме реального времени». Эта процедура позволяет использовать преимущества быстрого сбора и формирования доступных для поиска криминалистических данных с места преступления, таких как изображения лиц, полученные с электронных устройств или фотографий, быстро созданные профили образцов ДНК или электронная передача цифровых изображений отпечатков пальцев с места преступления непосредственно в AFIS для мгновенного поиска. В настоящее время стал возможным и становится все более привычным поиск и сопоставление имеющего доказательственное значение биометрического материала еще до окончания осмотра места преступления. Потенциально это может способствовать формированию оперативных данных криминалистической экспертизы, позволяющих оперативно установить личность подозреваемого либо определить или изменить направление следствия на ранних этапах расследования. В ходе расследования дел о терроризме это может помочь выявить новых подозреваемых или соучастников непосредственно после происшествия и предотвратить дальнейшие нападения. Очевидно, что этот потенциал можно еще больше нарастить, если массив биометрических данных, по которым проводится поиск в режиме реального времени, будет как можно более обширным.

Базы данных весьма полезны для расследования взрывов, устроенных террористом-смертником, когда останки террориста могут смешаться с останками жертв. В этих случаях крайне важно оперативно установить как личность террориста (для проведения расследования и предотвращения новых атак), так и личности жертв — в интересах их семей. ДНК, отпечатки пальцев и данные одонтологии (судебной стоматологии) являются основными биометрическими показателями, которые используются для идентификации жертв стихийных бедствий и катастроф[70].

6.2.2. На государственных границах

Как уже отмечалось ранее, биометрические мероприятия на границе делятся на две категории:

1) *биометрическая аутентификация (1:1)* — сопоставление биометрических данных, полученных от лица, совершающего поездку, на границе, с биометрическими данными, которые, например, хранятся в проездном документе, таком как электронный паспорт;

[70] Идентификация жертв стихийных бедствий и катастроф (DVI) — это признанная на международном уровне процедура выявления и идентификации жертв в случаях массовой гибели людей и оказания поддержки родным и близким погибших. Идентификация жертв осуществляется сотрудниками правоохранительных органов согласно процедуре, согласованной на международном уровне членами комитетов Интерпола по DVI. Интерпол также может оказывать непосредственную помощь и координировать действия в случае крупных и сложных международных инцидентов.

2) *поиск (1:n) по биометрическим спискам особого внимания* — поиск биометрических данных, полученных от лица, совершающего поездку, на границе или содержащихся в его электронном паспорте либо проездных документах, по спискам особого внимания, содержащим биометрические данные лиц, представляющих оперативный интерес, например находящихся в розыске, известных террористов или лиц, подозреваемых в терроризме, и т.д.

Каждая из этих процедур повышает эффективность оценки риска, связанного с совершающим поездку лицом, за счет управления идентификационными данными[71]. Оптимальной конфигурацией представляется проведение обеих процедур на границе. Аутентификация при пересечении границы подтвердит соответствие личности совершающего поездку лица сохраненным и подтвержденным биометрическим данным, однако в результате поиска по биометрическим спискам особого внимания может выясниться, что это лицо представляет оперативный интерес. Этот подход требует бóльших капиталовложений, но более высокие уровни гарантии и безопасности, которые он обеспечивает, обычно оправдывают дополнительные расходы.

Рисунок 5 подготовлен на основе *ICAO TRIP Guide on Border Control Management, Montreal (2018)*

(с разрешения ИКАО)

Списки особого внимания могут быть разными по объему и сложности содержания. Некоторые биометрические списки могут содержать отдельные базы данных, состоящие из эталонных данных, полученных от определенных категорий лиц, представляющих оперативный интерес. В другие биометрические контрольные списки в целях расширения их охвата могут добавляться отдельные биометрические данные с места преступления. Однако самая широкая интерпретация концепции списков особого внимания будет заключаться в объединении на законных основаниях всех национальных баз биометрических данных правоохранительных органов (см. раздел 6.3) в «национальный список особого внимания», пример которого приведен на рисунке 5. Это обеспечит оптимальный объем соответствующих данных для осуществления поиска по списку особого внимания, а также максимальную защиту совершающих поездки лиц и безопасность государства. Тем не менее на национальном уровне могут существовать нормативно-правовые ограничения, препятствующие реализации такого решения.

6.2.3. За пределами государственных границ

Страна может располагать зарубежными активами, которые считаются уязвимыми для атак террористов. Биометрия может быть важной составляющей любого плана, направленного на снижение угрозы. Так, речь может идти о требовании владеющей зарубежными объектами страны проводить проверку работающих на таких объектах, как, например, в посольстве, сотрудников — граждан страны размещения объекта. Для этого необходимо сотрудничество между обеими странами и, в идеале, заключение правомерного договора о поиске биометрических и биографических данных в базах данных обеих стран с целью убедиться в отсутствии у работников криминального прошлого или известной связи с террористами в любой из этих стран. Аналогично, в случае причастности граждан страны размещения объекта к террористической деятельности во владеющей объектом стране обмен биометрическими данными между этими странами и осуществление поиска по ним позволили бы обеим странам, во-первых, обеспечить защиту зарубежных активов страны — владелицы объекта, например коммерческих операций,

[71] Подробнее см. ICAO TRIP Guide on Border Control Management, Montreal (2018).

дипломатических представительств и мероприятий, а во-вторых, помочь стране размещения объекта выявить ее граждан, подозреваемых в террористической деятельности, и обеспечить их возвращение. Эта форма двустороннего сотрудничества и другие варианты обмена данными описаны в разделе 6.3.

6.2.4. Биометрические данные, полученные из военных источников

Некоторые страны используют свои воинские формирования для борьбы с терроризмом в пределах или за пределами своих национальных границ. В ходе таких операций биометрические данные часто используются для выявления террористов, которые могут попытаться скрыться и смешаться с местными жителями, чтобы избежать обнаружения или использовать их в качестве «живого щита». Военные могут использовать те же методы, что и правоохранительные органы, например развертывать мобильные или стационарные устройства сбора биометрических данных для получения эталонных образцов лиц, подозреваемых в терроризме, или проводить криминалистическую экспертизу предметов, изъятых у задержанных или в местах, представляющих оперативный интерес в связи с террористической или повстанческой деятельностью.

Биометрические данные, полученные в результате этих военных операций, могут также представлять особую ценность для правоохранительных органов в связи с их расследованиями дел о терроризме, однако при этом могут налагаться существенные ограничения на обмен такими данными и их использование, что в значительной степени будет зависеть от:

- правовых оснований для обмена такими биометрическими данными в соответствии с национальным законодательством и международными стандартами в области прав человека;
- приемлемости предоставленных военными биометрических данных и иных доказательств для гражданских судов;
- совместимости военных стандартов качества в области биометрии и криминалистической экспертизы со стандартами, применяемыми гражданскими властями данной страны.

В этом случае, даже если обмен данными и является правомерным, такие данные могут не соответствовать требуемым правовым стандартам для принятия в качестве доказательств, что не отменяет их значительной оперативной ценности (см. раздел 6.4).

Пример из практики 9. Аналитический центр по используемым террористами взрывным устройствам

Примером такого рода возможностей служит Аналитический центр по используемым террористами взрывным устройствам (TEDAC) Федерального бюро расследований США. TEDAC координирует усилия всех государственных органов, от правоохранительных органов до разведывательных служб и вооруженных сил, по сбору и обмену криминалистическими и оперативными данными в отношении устройств, тактики, методов и процедур обезвреживания и подрыва самодельных взрывных устройств (СВУ), установления связи устройств с их изготовителями и, самое главное, предотвращения новых атак. На сегодняшний день в TEDAC поступило более 100 000 образцов СВУ из более чем 50 стран. Отдел анализа биометрических данных (BAU) способствует укреплению глобального потенциала правительства США и международных партнеров по противостоянию угрозе СВУ и борьбе с ней за счет проведения своевременной высококачественной криминалистической экспертизы материалов СВУ на наличие скрытых отпечатков и следов ДНК, являющейся источником ценной оперативной информации для проведения расследования.

6.2.5. Гарантированная взаимная защита

Преимущества биометрических систем в области отслеживания и выявления террористов могут быть реализованы в полной мере только в случае сотрудничества и обмена данными на уровне стран. Страна может располагать всеобъемлющими и эффективными национальными биометрическими системами, действующими в пределах и за пределами ее границ, и даже входить в состав сложной региональной сети, однако, не имея доступа к касающимся терроризма данным из других стран, не входящих в такую национальную и региональную сеть, она остается потенциально уязвимой. Частичным решением проблемы служит обмен данными на национальном, двустороннем и региональном уровнях (см. раздел 6.3), однако для обеспечения взаимной защиты всех стран крайне важно наладить обмен биометрическими данными террористов на международном уровне, в мировом масштабе. Это также будет

способствовать воспрепятствию и пресечению деятельности террористов, которые могут временно находиться на территории стран с ограниченным или отсутствующим потенциалом регистрации биометрических данных, где они могут получить новые удостоверения личности или поддельные проездные документы, а затем отправиться инкогнито в другие пункты назначения. Чтобы противодействовать этой тактике и лишить террористов возможности сохранить анонимность или пользоваться «убежищами», откуда они могут вести свою деятельность, необходимо создать надежную и всеобъемлющую систему международного обмена биометрическими данными.

Хорошим примером глобальных возможностей такого рода служат базы биометрических данных Интерпола. Они выполняют эту жизненно важную защитную функцию путем предоставления странам возможностей для обмена биометрическими данными, имеющими отношение к терроризму, и, что особенно важно, подпадают под действие согласованных на международном уровне процедур управления, которые, в свою очередь, подлежат независимому надзору.

На рисунке 6 представлен широкий спектр *потенциальных* источников биометрических данных, имеющихся у национальных и международных государственных организаций, которые могут быть эффективно использованы для борьбы с терроризмом. Эти перечни баз данных не являются исчерпывающими, и доступность любой из них, естественно, зависит от нормативно-правовых ограничений на национальном уровне. Однако на рисунке показано, как теоретически можно объединить источники биометрических данных в целях взаимной защиты от террористической угрозы на национальном, региональном и глобальном уровнях.

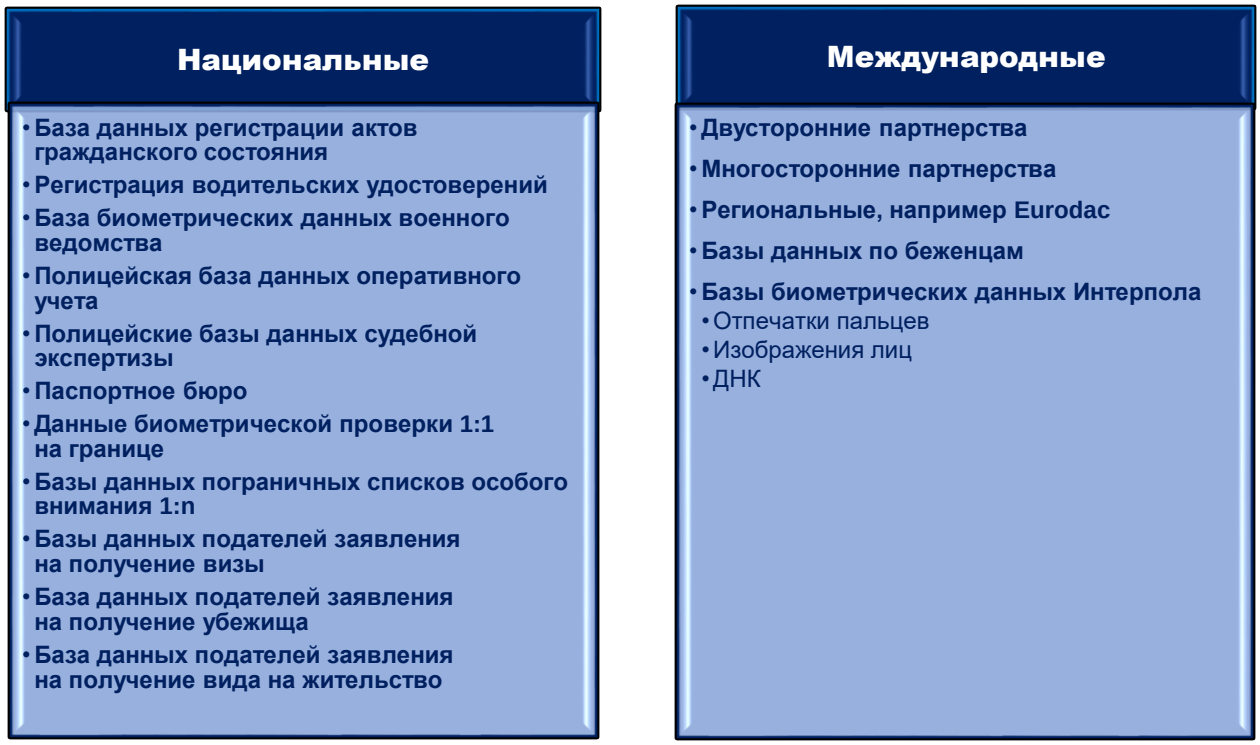


Рисунок 6. Источники биометрических данных

6.3. Протоколы обмена данными и правомерное объединение баз данных

По сложившейся традиции базы биометрических данных правоохранительных органов функционировали как «автономные» системы, поскольку каждое приложение служило для решения отдельных, конкретных рабочих задач и не было очевидных преимуществ обмена данными между этими системами. Эти базы данных были разработаны специально для выполнения рабочих функций, связанных с охраной правопорядка, пограничным контролем или местами лишения свободы. Однако возросшая за последние десятилетия угроза глобального терроризма вынудила многие правительства пересмотреть способы использования своих баз данных и методы обмена данными для обеспечения более эффективной защиты своих граждан. Это повысило способность к взаимодействию и операционную совместимость баз

данных на национальном уровне, а также обеспечило развитие двусторонних, многосторонних и региональных сетей баз данных и их объединение на международном уровне. Этот процесс, начавшийся с объединения разрозненных одномодальных баз данных, привел к появлению в некоторых странах и регионах ультрасовременных взаимозаменяемых сетей, состоящих из взаимосвязанных мультимодальных баз данных, предназначенных для выполнения целого ряда оперативных задач в области охраны правопорядка, пограничного контроля и других государственных функций как на национальном, так и на международном уровне. К взаимодействию такого типа предъявляются перечисленные ниже требования.

Рисунок 7. Требования к взаимодействию сетей биометрических данных

Критерии выбора сети. Владельцам баз биометрических данных следует рассмотреть свое членство в сети биометрических данных исходя не только из собственных бизнес-требований и оперативных целей, какими бы важными они ни были, но и в более широкой перспективе, принимая во внимание потенциальные дополнительные преимущества как для своей страны или региона, так и для остальных партнеров по сети. Этот подход является необходимым и основополагающим при объединении в сеть баз биометрических данных для борьбы с терроризмом. Маловероятно также, что владельцы баз биометрических данных, имеющие намерение присоединиться к международной сети, рискнут поделиться своими данными с недобросовестными или ненадежными партнерами, и этот вопрос должен быть надлежащим образом урегулирован любой крупной международной сетью, например, см. раздел 6.1.3 «Приложения, применяемые Интерполом».

Управление и регулирование. Сети биометрических данных должны функционировать в правовых рамках, позволяющих передавать биометрические данные и иные связанные с ними метаданные. Каждая существующая база данных уже должна функционировать в соответствии с национальным законодательством и нормами международного права в области прав человека, однако для осуществления поиска между различными базами данных как внутри одной страны, так и на международном уровне могут потребоваться дополнительные законодательные меры. Применительно к международным сетям этот вопрос обычно решается путем заключения официальных соглашений, таких как меморандумы о взаимопонимании, между участвующими субъектами или странами. Правомерное осуществление поиска может быть ограничено одиночными поисковыми запросами по каждому конкретному случаю (например, по конкретным преступлениям) или применяться более широко, например в виде автоматического поиска по всем данным, имеющимся в этой сети.

Нормативно-правовая база должна обеспечивать независимый надзор за работой всей сети и уделять особое внимание функциям управления данными и целям использования этих данных, с тем чтобы не

допустить любого несанкционированного расширения области применения, например поиска по массивам данных внутри сети или за ее пределами, доступ к которым запрещен законом или действующими операционными протоколами. В некоторых странах для выполнения этих функций назначают должностных лиц, например уполномоченных или комиссаров по биометрии. Кроме того, имеются регуляторные органы, такие как британский регуляторный орган в области криминалистической экспертизы, которые отвечают за надзор над научными процессами, включая процессы создания экспертно-криминалистических биометрических данных и профилей, используемых в этих базах данных. Таким образом, и функционирование базы данных, и экспертно-криминалистические данные, которые она содержит, подлежат независимому контролю и надзору, включая деятельность комитетов по экспертизе этических норм или аналогичных органов (см. раздел 5.1.2).

Оценка защиты данных и воздействия на неприкосновенность частной жизни — см. разделы 5.2.3 и 5.2.4.

Владение данными. Каждая биометрическая запись должна иметь определенного владельца данных (см. раздел 5.2.6), который в соответствии с законодательством несет ответственность за регистрацию, использование, сохранение и удаление этих данных. Это имеет особое значение при работе с сетью баз биометрических данных, содержащих большие объемы данных из разнообразных источников.

Передача данных по сети и безопасность. Поток биометрических данных и иной информации должен быть эффективным и своевременным. Учитывая характер данных, которые содержатся в сети, она должна быть надежной и иметь надлежащий уровень безопасности для обеспечения защиты сотрудников и операционной среды, в том числе данных, аппаратных средств, программного обеспечения и сети передачи данных. Надлежащей практикой считается сохранение в сетевой системе только биометрических данных. Персональные, биографические данные, связанные с соответствующими биометрическими данными, следует хранить в отдельной системе. Эти меры предосторожности позволяют предотвратить доступ к личной информации и биометрическим данным из одного приложения. В связи с этим биометрическим данным обычно присваивают уникальный идентификационный номер, чтобы при необходимости их можно было связать с соответствующими биографическими данными, используя безопасные рабочие процедуры.

Протоколы поиска. Сеть должна быть обеспечена синхронизированными систематическими списками очередности поиска и протоколами передачи файлов, контролирующими время и последовательность каждого поиска, чтобы гарантировать, что поиском охвачены все наборы данных во всех базах данных сети, т.е. ничто не было пропущено даже в периоды пикового спроса (см. ниже подраздел «Объединенные в сеть базы биометрических данных: протоколы поиска»).

Стандарты биометрических данных. Поиск по сети может быть выполнен только в том случае, если партнеры предоставляют биометрические данные совместимого типа. Например, в разных частях света, в частности в Австралии, Европе и США, для ДНК-профилирования используются различные наборы реагентов. Каждый из этих наборов реагентов используется в отношении конкретных и уникальных STR-локусов в дополнение к STR-локусам, которые являются общими для всех. Однако наличие достаточного количества общих локусов позволяет вести поиск по профилям, созданным с использованием различных наборов реагентов, в любой базе данных ДНК. Новейшие наборы реагентов для профилирования используются в отношении еще большего количества STR-локусов, за счет чего пропорционально возрастает число локусов, являющихся общими для всех партнеров.

В основе всех рабочих характеристик сети должны лежать технические и научные стандарты (например, ISO 17025), которые описаны в разделе 5.4.

Стандарты передачи данных. Не соответствующее стандартам качество изображения может подвергнуть систему биометрических данных риску возникновения серьезных и ненужных ошибок, таких как увеличение количества ложных отказов или даже ошибочных идентификаций. Чтобы гарантировать сохранение качества изображений, таких как изображения лица или отпечатки пальцев, во время передачи по сети, следует использовать[72] стандарты, содержащие требования к разрешению изображения. Это означает, что изображение будет оставаться ясным и четким вне зависимости от того, в каком месте сети оно рассматривается.

[72] Например, NIST Special Publication 1152 ‘Latent Interoperability Transmission Specification’ www.nist.gov.

Управление предварительными и окончательными результатами. Совпадения биометрических данных, установленные по итогам поиска по сети (предварительные результаты), и действия, предпринимаемые как следствие этих совпадений (окончательные результаты), необходимо тщательно контролировать в соответствии с требованиями законодательства, жесткими научными стандартами и строгими организационными процедурами (см. раздел 6.4). В рамках системы менеджмента качества следует провести экспертную проверку совпадений биометрических данных с участием другого эксперта или, предпочтительно, двух экспертов, прежде чем будут выданы результаты. Это предотвращает риск того, что один человек может допустить ошибку идентификации.

Объединенные в сеть базы биометрических данных: протоколы поиска. Существуют два основных метода синхронизации поиска между базами данных.

Односторонний поиск. Биометрические данные (a) регистрируются в базе данных 1, после чего по этой базе проводится поиск. Если совпадения не обнаружены, данные сохраняются в базе данных 1 и направляются в базу данных 2 для поиска и, в случае повторного отсутствия совпадений, сохраняются в базе данных 2.

Примечание. Возможные совпадения могут быть пропущены, если данные (a) используются *только* для поиска и *не* сохраняются в базе данных 2, поскольку результат поиска будет ограничен только непосредственным временем поиска. Например, если в дальнейшем данные для поиска (b), которые совпадают с биометрическими данными (a), регистрируются и используются для поиска в базе данных 2 *после* того, как был осуществлен поиск по данным (a), совпадения не будут обнаружены, потому что данные (a) не были сохранены и, соответственно, не используются для поиска данных (b). Таким образом, при однонаправленной передаче данных между двумя и более базами данных важно обеспечить сохранение этих данных после поиска в каждой базе данных, чтобы гарантировать их обнаружение при последующих поисках и, таким образом, поддерживать непрерывный охват.

В случае однонаправленной передачи данных управление данными также может вызывать проблемы, особенно если базы данных относятся к различным юрисдикциям или странам. Каждый владелец данных должен заключить с другими партнерами официальное соглашение относительно времени хранения и политики удаления совместно используемых данных. В отсутствие такого соглашения владельцы других баз данных не обязаны исполнять эти требования, поскольку, возможно, на них не распространяются те же законы, что и на исходную базу данных. Их нежелание выполнять запросы на удаление данных может объясняться и другими причинами, такими как финансовые, ресурсные или временны*е* ограничения.

Взаимный двусторонний поиск. Биометрические данные (a) регистрируются в базе данных 1, после чего по этой базе данных осуществляется поиск. Если совпадения не обнаружены, данные сохраняются в базе данных 1 и направляются в базу данных 2 для осуществления поиска, но при этом данные (a) не сохраняются в базе данных 2. Аналогичным образом, если биометрические данные (b) регистрируются в базе 2 и сопоставляются с имеющимися в ней данными, а затем направляются для осуществления поиска в базу данных 1, в базе данных 1 они не сохраняются. Этот метод воспроизводится для любого количества баз данных в сети, поскольку каждая база данных осуществляет поиск вновь зарегистрированных у себя данных по всем остальным базам данных. Риск пропуска возможных совпадений (как при одностороннем поиске) устраняется путем внесения данных в исходную базу данных *до* осуществления поиска по всей сети с целью предотвратить разрывы во времени, что в противном случае позволило бы одновременно входящим поисковым сетевым запросам разминуться друг с другом.

Примечание. Эту систему часто называют многократным поиском с одной регистрацией или «введи один раз — ищи, сколько хочешь». База, которой принадлежат эти данные, сохраняет их после поиска, но все остальные базы данных используют их только для поиска. Это упрощает управление данными, поскольку данные владельца хранятся только в его базе данных, а также сокращает объем передаваемых по сети данных. Последовательность поиска между базами данных должна быть под строгим контролем, особенно когда данные из нескольких баз данных, относящихся к одной юрисдикции, передаются в базу данных, относящуюся к другой юрисдикции. Например, все комбинации поиска по базам данных юрисдикции (1) должны быть полностью выполнены, прежде чем какая-либо из них отправит поисковый запрос в юрисдикцию (2), поскольку в противном случае в юрисдикции (2) могут быть обнаружены совпадения, которые должны были быть обнаружены еще в юрисдикции (1). Этого можно избежать, направляя поисковые запросы из юрисдикции (1) в юрисдикцию (2) через единый управляемый канал.

6.3.1. Прогностическая биометрия: превентивное использование сетей баз биометрических данных для предотвращения террористических атак

Объединение баз биометрических данных из широкого спектра источников в сфере охраны правопорядка и пограничного контроля (а также военных биометрических данных, если таковые имеются) позволяет анализировать коллективные результаты работы сети не только с точки зрения отдельных оперативных потребностей, таких как раскрытие преступлений или проверка с целью установления личности на границе и т.д., но и в виде более широкого ряда или модели «биометрических событий» как таковых. Что касается террористической угрозы, то каждое событие может иметь к ней прямое или косвенное отношение либо, возможно, выглядеть совершенно безобидно и не иметь очевидной значимости, однако рассмотренное в контексте другой информации или других биометрических событий, оно может в значительной степени способствовать созданию широкой оперативной картины перемещений и деятельности террористов. Некоторые из этих результатов могут быть достаточно очевидными, например выявление подозрительной подготовки к поездке или установление связи с преступлениями террористического характера, другие же, хотя и менее заметные и не столь прямолинейные, также могут служить ценными указателями, если оценивать их вместе с другими соответствующими материалами. Этот метод, представленный на рисунке 8 ниже, предусматривает традиционное реагирующее и, в значительной степени, пассивное использование баз биометрических данных в следственных целях с задачей спасти человеческие жизни путем предотвращения террористических атак до их совершения за счет превентивного использования биометрических данных из самых разных источников вместе с другими оперативными материалами.

Рисунок 8. Прогнозная модель использования биометрических данных

Традиционные базы биометрических данных (описаны в разделе 4) разрабатывались как системы реагирующего действия и были призваны ответить на связанные со следствием вопросы на основании идентификационных данных и *нынешних* или *прежних* действий, такие как *«Известно ли нам, кто вы, кто ваши сообщники, и что вы делали раньше?»*. Объединенные системы биометрических данных, безусловно, также могут отвечать на эти вопросы, однако их можно использовать и превентивно для построения предположений и прогнозирования потенциальных будущих действий и ассоциаций, т.е. «*Что вы и ваши сообщники планируете или, вероятно, будете делать, где и когда?»*. Таким образом, необходимо проведение всестороннего и тщательного анализа всех результатов, полученных во всей сети,

поскольку в сочетании с другой оперативной информацией это может стать решающим фактором успеха в сфере оценки и предотвращения террористической деятельности. Это в равной степени относится и к последующему управлению окончательными результатами.

6.4. Управление окончательными результатами

6.4.1. Контекстуальная оценка предварительных результатов

В автономных системах биометрических данных получение предварительных результатов может быть в значительной степени автоматизировано, а участие человека сведено к минимуму (см. раздел 4), однако когда данные, содержащиеся в этих системах, интегрируются в сеть многофункциональных баз биометрических данных и используются для перекрестного поиска, абсолютно необходимой становится тщательная проверка и изучение полученных предварительных результатов до принятия каких бы то ни было мер. Контекстуальная оценка предварительных результатов и управление окончательными результатами должны проводиться с учетом следующих факторов.

Обеспечение правомерных и соразмерных ответных мер и решение проблемы ошибочной или косвенной идентификации. Для специалистов, которые получают и обрабатывают результаты поиска по базам биометрических данных любого типа, в особенности если база данных имеет отношение к терроризму, естественным является формирование негативного мнения и предположение, что любое лицо, идентифицированное этой системой, обязательно является террористом. Однако это не всегда оказывается верно по следующим причинам:

1) в результате человеческой или системной ошибки то или иное лицо может быть неправильно идентифицировано, и хотя это очень редкое явление, оно должно являться неотъемлемой частью любого регламента контрольных процедур, особенно если другие данные или доказательства вызывают сомнения в правильности полученного результата;
2) у правительств или иных сторон может возникнуть желание использовать предварительные результаты поиска биометрических данных ненадлежащим образом, выдвигая ложные обвинения в терроризме в целях подрыва деятельности оппозиции, политических активистов или правозащитников (см. раздел 5.2.5);
3) идентифицированное лицо может быть совершенно не причастно к терроризму. Поэтому контекстуальная и относительная значимость любого результата должна подвергаться тщательной оценке *до* применения каких-либо мер.

Например, предмет или место, являющиеся ключевыми в расследовании дела о терроризме, могли быть случайно «загрязнены» кем-либо, не имеющим отношения к террористической деятельности, или же осторожным сотрудником правоохранительных органов. Затем эксперты-криминалисты и судебные эксперты собирают материалы для криминалистической экспертизы и вносят данные о них в соответствующую сеть баз данных. Эти «побочные» данные могут затем отзываться на поисковые запросы по всей сети и являться источником совпадения, например когда соответствующее лицо впоследствии предоставляет свои биометрические данные для пересечения границы. Поэтому при принятии действий сотрудники органов пограничного контроля должны учитывать весь контекст любого совпадения биометрических данных, а не исходить из автоматического предположения о том, что человек является террористом, только из-за совпадения биометрических данных. Ответные меры правоохранительных органов должны быть взвешенными и соответствующими нормам международного права в области прав человека. Эти процедуры контекстуальной оценки должны быть предметом тщательного независимого надзора для предотвращения любого потенциально неправомерного задержания или возможной судебной ошибки.

Коммуникационная стратегия. Чтобы обеспечить последовательное и эффективное применение контекстуальных оценок при управлении окончательными результатами, власти должны создать четкие, безопасные и непрерывные линии коммуникаций между теми, кто занимается оценкой предварительных биометрических результатов, и оперативными сотрудниками и руководителями, которые должны будут действовать на основании полученной информации. Для этого необходимо наладить ускоренный диалог между владельцами данных с места преступления (правоохранительными органами) и сотрудниками, непосредственно работающими с лицом, задержанным в связи с совпадением его данных с данными с места преступления. Обмен информацией этого и других видов распространен довольно широко и, как правило, представляет собой стандартную рабочую процедуру в национальных и международных правоохранительных кругах. Необходимо также, чтобы в рамках коммуникационной сети определялась

приоритетность результатов поиска по базам данных и обеспечивалось соблюдение согласованных сроков, особенно в случае ареста или задержания каких-либо лиц вследствие совпадения биометрических данных. Коммуникационная стратегия также должна предусматривать наличие полного списка получателей предварительных результатов поиска биометрических данных в сети и установление критериев урегулирования конфликтов для предотвращения или разрешения споров между двумя получателями по таким вопросам, как примат юрисдикции или следственные приоритеты.

Модальности, стандарты представления криминалистических данных и научные интерпретации. Некоторые сети баз биометрических данных могут использовать только одну модальность, однако более обычным и эффективным является использование нескольких модальностей, работа с которыми осуществляется параллельно в рамках сети биометрических данных, например поиск по отпечаткам пальцев, ДНК и изображениям лиц. Результаты поиска с помощью мультимодальных систем дают самое широкое представление о деятельности, если сочетаются с многофункциональными системами, содержащими криминалистические данные с мест преступлений, а также эталонные данные из различных источников. Криминалистические материалы, полученные с места преступления, не всегда могут «полностью» совпадать с эталонными данными по причинам, описанным в разделе 4.5, и тем не менее они могут представлять огромную доказательную ценность для расследования. Важно, чтобы специалисты, которые занимаются сведением воедино предварительных результатов поиска по базе данных, в полной мере понимали и оценивали оба компонента. Оценка относительной убедительности совпадения и его потенциальной доказательственной или следственной ценности вместе с любой другой соответствующей информацией, полученной в ходе контекстуальной оценки, должны быть сведены воедино и представлены соответствующему должностному лицу, следователю или аналитику, которые таким образом получают возможность принять надлежащие и соразмерные меры. Поэтому целесообразно осуществлять регистрацию лишь тех данных, которые могут быть представлены в качестве доказательств в суде. Это позволяет в полной мере использовать все совпадения в ходе расследования и обнародовать или представлять их в суде.

Пример из практики 10. Процедуры управления выпуском уведомлений Интерпола

Практический пример управления международным обменом данными

Несмотря на то что принятая Интерполом система уведомлений с красным углом не связана с результатами поиска биометрических данных, существует явная параллель между ней и процессом оценки, описанным в разделе 6.4.1, а кроме того, она представляет собой эффективную модель управления данными в глобальном масштабе. Она должна в обязательном порядке функционировать в соответствии с нормами международного права и правилами Интерпола и гарантировать наличие эффективного механизма коммуникации между ключевыми сторонами и системы независимого и тщательного рассмотрения жалоб и апелляций лиц, в отношении которых выпущено уведомление с красным углом.

Уведомление с красным углом — это запрос на предварительный арест лица, ожидающего решение об экстрадиции, который выпускается Генеральным секретариатом Интерпола по запросу страны-члена на основании действующего национального ордера на арест. Уведомления с красным углом также могут быть выпущены по запросу международного трибунала.

Помимо уведомлений с красным углом, Интерпол выпускает и другие виды уведомлений, например уведомление с синим углом, которое выпускается по запросу страны-члена в целях поиска информации, связанной с уголовным расследованием. Государства-члены могут также осуществлять рассылки, которые представляют собой запросы о сотрудничестве, распространяемые непосредственно между странами-членами.

Интерпол не может настаивать или принуждать страну-член арестовать лицо, в отношении которого выпущено уведомление с красным углом. Также Интерпол не может требовать от страны-члена совершения каких-либо действий в ответ на запрос другой страны-члена. Каждая страна — член Интерпола сама решает вопрос о придании уведомлению с красным углом той или иной юридической значимости на своей территории. Принимая решение действовать на основании уведомления или какого-либо иного запроса, страна полностью принимает на себя ответственность за это решение. Оперативная эффективность соглашений об уведомлениях с красным углом зависит от способности механизма передачи данных между национальными центральными бюро (НЦБ) функционировать в круглосуточном и круглогодичном режиме.

Все уведомления и рассылки должны соответствовать правилам и предписаниям Интерпола. К ним относится статья 2 Устава Интерпола, где содержится прямая ссылка на дух Всеобщей декларации прав человека, и статья 3 Устава Интерпола, согласно которой «организации категорически запрещается осуществлять какое-либо вмешательство или деятельность политического, военного, религиозного или расового характера». В правилах Интерпола по обработке данных содержатся дополнительные критерии для выпуска каждого типа уведомлений, а также информация о распределении обязанностей между различными сторонами, т.е. запрашивающей страной, Генеральным секретариатом, странами-получателями и т.д.

Надзор со стороны контролирующих органов. Существует несколько уровней контроля, направленных на обеспечение соблюдения нормативных правил Интерпола. К первому уровню относятся НЦБ, которые направляют запрос на сотрудничество с органами полиции (например, запрос на выпуск уведомления с красным углом). Они несут полную ответственность за любую информацию, которую они вносят в базы данных Интерпола или распространяют через информационную систему Интерпола. Они должны обеспечить точность, уместность и актуальность информации, а также соответствие обработки этой информации Уставу Интерпола и их внутреннему законодательству.

Вторым уровнем является штаб-квартира Генерального секретариата Интерпола. В ноябре 2016 года Генеральный секретариат создал специальную целевую группу, включающую междисциплинарное подразделение, в состав которого вошли юристы, сотрудники полиции, аналитики и специалисты-практики, для контроля за обработкой данных на всех уровнях, в том числе применительно к уведомлениям с красным углом и рассылкам. Целевая группа тщательно проверяет все запросы на предмет их соответствия Уставу или правилам Интерпола. В процессе рассмотрения целевая группа может запросить дополнительную информацию из всех соответствующих источников, с тем чтобы принять решение о выпуске уведомления или отказе в его выпуске. Кроме того, страна-член может выразить озабоченность в отношении информации, обработка которой осуществляется другой страной-членом, включая выпуск уведомления с красным углом, если она полагает, что это было сделано в нарушение правил Интерпола.

Вопросы беженцев. В июне 2014 года Интерпол внедрил новую политику в отношении дел, касающихся беженцев. Это дает Интерполу возможность оказывать странам-членам поддержку в предотвращении злоупотребления статусом беженцев со стороны преступников, обеспечивая при этом адекватные и эффективные гарантии защиты прав беженцев. Каждый запрос на выпуск уведомления с красным углом или рассылки в отношении беженца оценивается Генеральным секретариатом или, в соответствующих случаях, Комиссией по контролю за файлами Интерпола (см. раздел 6.1.3), в индивидуальном порядке. Как правило, выпуск уведомлений с красным углом и рассылок в отношении беженцев не допускается в том случае, если статус беженца или лица, ищущего убежища, подтвержден, а запрос на уведомление или рассылку исходит от страны, в которой данное лицо опасается преследования.

Права лиц, в отношении которых выпущено уведомление или рассылка. Решение о выпуске уведомления или внесении информации в базу данных Интерпола не оказывает влияния на права человека, включая его право считаться невиновным, право оспаривать дело в соответствующих органах власти страны, выдавшей ордер на арест и запрашивающей помощь Интерпола, или право оспаривать дело в национальных органах, рассматривающих запрос об экстрадиции.

У соответствующего лица есть как минимум три возможности для оспаривания выпущенного в отношении него уведомления или рассылки:

- оспорить свое дело в национальных органах страны, выдавшей запрос, либо непосредственно, либо путем найма законного представителя. Поскольку уведомление с красным углом выпускается на основании действительного ордера на арест, в случае если ордер на арест будет отозван компетентными национальными органами, уведомление с красным углом будет удалено;
- связаться с Комиссией по контролю за файлами Интерпола;
- обратиться к своей стране с просьбой принять дело к производству и выразить протест против выпуска уведомления с красным углом.

В случае отмены уведомления с красным углом или рассылки по любой причине всем странам-членам направляется уведомление об этом решении и предлагается удалить всю соответствующую информацию из их национальных баз данных.

Эти меры защиты обеспечивают прозрачный и структурированный процесс решения таких вопросов и позволяют избежать потенциального неправомерного использования уведомлений с красным углом.

6.4.2. Стратегические цели и руководящие указания по проведению расследований

Национальные и региональные контртеррористические стратегии должны отражать значимость криминалистики и биометрии. Органы охраны правопорядка и службы пограничного контроля должны активно поддерживать такие стратегии, используя все имеющиеся у них криминалистические и биометрические ресурсы и обеспечивая эффективность функционирования баз данных.

Криминалистические и биометрические стратегии могут также осуществляться на уровне расследования, и эту практику следует поощрять путем проведения обучения и выработки оперативной доктрины. В задачу старшего следователя, руководящего расследованием дела о терроризме, входит определение в начале расследования основных криминалистических и биометрических целей, причем применительно к биометрии обычно необходимо придерживаться следующих принципов:

- все эталонные биометрические образцы арестованных, полученные в ходе расследования, должны быть оптимального качества;
- все места преступлений должны подвергаться всесторонней, строго последовательной криминалистической экспертизе для сбора максимально возможного количества образцов ДНК и отпечатков пальцев в целях установления более широкого круга связей террористов в дополнение к конкретным криминалистическим потребностям данного расследования;
- все соответствующие биометрические данные, полученные в ходе расследования, должны быть зарегистрированы и/или проверены на наличие совпадений во всех соответствующих национальных и международных базах данных.

Эти три элемента биометрической стратегии решают следующие вопросы:

1) *удовлетворение потребностей расследования*, т.е. получение высококачественных биометрических эталонных данных для эффективного сопоставления по модели 1:1 с материалами с места преступления, их регистрация и проведение поиска по базам данных для продвижения в расследовании;
2) *удовлетворение потребностей расследования других дел о терроризме и оперативно-разыскных мероприятий* за счет более широкого охвата мест преступления и сбора биометрических материалов, которые могут не относиться напрямую к основному расследованию, однако могут способствовать выявлению неизвестных ранее соучастников, ячеек или сетей;
3) биометрические данные, собранные в ходе одного расследования, могут не только способствовать раскрытию или установлению связей с другими расследованиями, но также потенциально могут *предотвратить будущие террористические атаки* и тем самым спасти жизни многих людей.

Практические рекомендации по разделу 6

6a Государства должны противодействовать угрозе, создаваемой постоянными перемещениями террористов через международные границы, используя биометрические системы для защиты своих границ и национальных активов и осуществляя законный обмен биометрическими данными с международными партнерами.

6b Обеспечение безопасности границ можно сделать более эффективным за счет применения методов биометрической верификации 1:1 в сочетании с поиском 1:n по биометрическим спискам особого внимания для отслеживания и выявления террористов и их сообщников. Масштаб биометрических списков особого внимания может быть любым — от небольшой подборки справочного характера до списка, полностью совместимого с базами данных правоохранительных органов по управлению идентификационной информацией и раскрытию преступлений, с учетом положений национального законодательства, нормативных ограничений и международного права в области прав человека.

6c Чтобы противостоять угрозе терроризма и угрозе со стороны иностранных боевиков-террористов, государствам настоятельно рекомендуется в максимальной степени использовать базы биометрических данных Интерпола (изображения лица, отпечатки пальцев и ДНК).

6d Обмен биометрическими данными на международном уровне является крайне важным инструментом борьбы с терроризмом, однако он должен осуществляться в соответствии с международным правом в области прав человека. Правительства должны сделать все необходимое для того, чтобы, осуществляя обмен биометрическими данными, они не способствовали арестам, которые приведут к пыткам или смертной казни.

6e Крайне важно до принятия каких-либо мер тщательно и полностью изучить контекст всех совпадений биометрических данных, обеспечив при этом полное соблюдение норм международного права в области прав человека.

6f Национальные и региональные стратегии борьбы с терроризмом должны отражать значимость криминалистики и биометрии, возлагая на органы охраны правопорядка и службы пограничного контроля обязанность обеспечивать в максимальном объеме законный сбор и использование криминалистических или биометрических материалов и поддержание эффективности баз данных и протоколов обмена данными.

Справочные материалы к разделу 6

ICAO TRIP Guide on Border Control Management, Montreal (2018)

PNRGOV EDIFACT & XML Message Implementation Guide:
www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx

Рекомендации ВТамО/ИАТА/ИКАО в отношении записей регистрации пассажиров (Doc 9944)

ИКАО Doc 9303 — Машиносчитываемые проездные документы

www.interpol.int/INTERPOL-expertise/I-Checkit

www.interpol.int/INTERPOL-expertise/Databases

The INTERPOL DNA Gateway — Official Publication February 2017

The INTERPOL Facial Images Best Practices Guide October 2015 & Facial Recognition Fact Sheet

INTERPOL Guidelines concerning Fingerprint Transmission 2012

INTERPOL Rules on the processing of information for the purposes of international police co-operation

ETIAS http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282017%29583148

www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system

www.consilium.europa.eu/prado/en/check-document-numbers/check-document-numbers.pdf

www.un.org/sc/ctc/

https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/fact-sheets/docs/20161116/factsheet_-_etias_en.pdf

http://europa.eu/rapid/press-release_MEMO-16-3706_en.htm

NIST Special Publication 1152 ‘Latent Interoperability Transmission Specification’ www.nist.gov

7. Добавления

7.1. Сокращения

АСПК	автоматизированная система пограничного контроля	AFIS	автоматизированная система идентификации отпечатков пальцев
ВИС	визовая информационная система	API	предварительная информация о пассажирах
ИБТ	иностранные боевики-террористы	CCF	Комиссия по контролю за файлами Интерпола
ИКАО	Международная организация гражданской авиации	EER	уровень равной вероятности ошибок
ИОК	инфраструктура открытых ключей	ETS	электронные системы авторизации поездок
ИСО	Международная организация по стандартизации	FAR	вероятность ложного допуска
ИСПК	информационная система пограничного контроля	FRR	вероятность ложного недопуска
МСЗ	машиносчитываемая зона	FTA	вероятность отказа сбора данных
МЭК	Международная электротехническая комиссия	iAPI	Интерактивная предварительная информация о пассажирах
ППГ	пункт пересечения границы	LDS	логическая структура данных
СУК	система управления качеством	PNR	система учетных записей пассажира
ШИС	Шенгенская информационная система	STR	короткие тандемные повторы
э-ИСПК	электронная информационная система пограничного контроля	TAR	вероятность правильного допуска
		TRR	вероятность правильного недопуска

7.2. Словарь биометрических терминов

Аккредитация — согласно определению ИСО, аккредитация — это «официальное признание независимым органом, более известным как орган по аккредитации, что сертифицируемый орган действует в соответствии с международными стандартами».

Автоматизированная система идентификации отпечатков пальцев — электронная система, предназначенная для хранения и поиска больших объемов 1) эталонных наборов отпечатков пальцев и ладоней и 2) отпечатков пальцев и ладоней с мест преступлений. Поиск по идентификационным данным обычно выявляет одно совпадение либо дает отрицательный результат. Результаты поиска в процессе расследования преступления представлены в виде списка возможных совпадений. Результаты проверяются экспертом-дактилоскопистом, который подтверждает совпадения, выявленные системой.

Биометрическая модальность — тип биометрических данных, используемый в системном или операционном контексте, например отпечатки пальцев, изображения лица, радужная оболочка глаза и т.п.

Сертификация — согласно определению ИСО, сертификация — это «предоставление независимым органом письменного удостоверения (сертификата), согласно которому рассматриваемый продукт, услуга или система соответствуют определенным требованиям».

Оценка соответствия — согласно определению МЭК, оценка соответствия — это «демонстрация соблюдения определенных требований, предъявляемых к продукту, процессу, системе, лицу или органу».

Поиск в процессе расследования преступления — двунаправленный протокол поиска, в ходе которого осуществляется поиск совпадений 1) эталонных данных с данными с места преступления и 2) данных с места преступления с эталонными данными.

Данные с места преступления — сформированы из образцов и предметов, собранных на месте преступления.

Уровень равной вероятности ошибок (EER) — определенное пороговое значение, при котором вероятность ложного допуска и вероятность ложного недопуска равны.

Обработка исключений — чрезвычайные меры, которые используются в случае сбоя биометрической системы, например вмешательство человека, резервная система и т.д.

Вероятность отказа сбора данных (FTA) — это доля всех зафиксированных транзакций, которые не удалось завершить из-за сбоев на стадии представления данных (не было получено изображение), выделения характерных признаков или контроля качества.

Вероятность ложного допуска (FAR) — это доля случаев ложного допуска в общем числе запросов на биометрическую идентификацию, которые должны были быть отвергнуты, т.е. доля несовпадений, *которые система определила и представила как совпадения*, в общем числе истинных несовпадений.

Вероятность ложного недопуска (FRR) — это доля ложного недопуска в общем числе запросов на биометрическую идентификацию, которые должны были быть приняты, т.е. доля совпадений, *которые система определила и представила как несовпадения*, в общем числе истинных совпадений.

Идентификация (известная также как сопоставление одного со многими, или 1:n). В этом случае поиск ведется без опоры на предполагаемые идентификационные атрибуты, и поэтому вся база данных изучается на предмет возможного совпадения.

Поиск по идентификационным данным — определяет, было ли лицо ранее зарегистрировано в базе данных, путем сопоставления эталонных биометрических данных этого лица со всеми эталонными данными, хранящимися в системе.

Морфинг — слияние биометрических образцов (например, изображений лиц), принадлежащих двум и более донорам, с тем чтобы обеспечить успешную верификацию любого из таких доноров на основе «преобразованных» идентификационных данных.

Система управления качеством — официальный протокол, определяющий и документирующий процессы, процедуры и сферы ответственности для достижения целей по качеству. Система предназначена для координации и руководства деятельностью организации, направленной на удовлетворение клиентских и нормативных требований, устранение несоответствий и формирование культуры непрерывного совершенствования.

Эталонные данные собираются в контролируемых условиях у арестованных или подозреваемых в совершении правонарушения. К числу таких данных относятся, например, отпечатки всех 10 пальцев рук, снятые электронным сканером или традиционным способом с использованием чернил и бумаги; ротовые мазки, взятые с внутренней стороны щеки арестованного, образцы волос или крови, которые затем обрабатываются для получения полного ДНК-профиля; цифровые фотографии лица и т.п.

Поиск в случае серийных преступлений/происшествий — поиск биометрических или криминалистических данных с места преступления по базе данных, содержащей аналогичные данные с места преступления для выявления любых совпадений, что позволяет установить связь между различными преступлениями или событиями в рамках одного расследования.

Спуфинг (известный также как представление ложного идентификатора) — это представление фальсифицированных биометрических данных легального зарегистрированного пользователя (например, латексной маски, фотографии, поддельного отпечатка пальца или поддельной записи голоса) для получения несанкционированного доступа к биометрической системе идентификации.

Пороговое значение — регулируемый параметр биометрических систем. Устанавливает баланс между допуском и недопуском для конкретной заявки.

Пропускная способность — количество лиц, использующих биометрическую систему в течение определенного промежутка времени.

Вероятность правильного допуска (TAR) — показатель способности системы правильно сопоставить признаки биометрической идентичности одного и того же лица.

Вероятность правильного недопуска (TRR) — показатель количества случаев, когда было правильно установлено *несовпадение* признаков биометрической идентичности одного лица с признаками биометрической идентичности других лиц, внесенных в базу данных, т.е. частота случаев правильного несовпадения.

Верификация (известная также как сопоставление одного с одним, или 1:1). В этой модели предложенные идентификационные атрибуты применяются для того, чтобы выбрать из базы данных только один шаблон и сопоставить его с рассматриваемым шаблоном. По сути, это процесс аутентификации, в ходе которого проводится сопоставление рассматриваемого шаблона с шаблоном из базы данных и либо подтверждается, что оба шаблона соответствуют одному и тому же лицу, либо это не подтверждается.

7.3. Указатель международных организаций

Институт биометрии www.biometricsinstitute.org

Международная организация гражданской авиации www.icao.int

Международный комитет Красного Креста www.icrc.org

Международная организация уголовной полиции (Интерпол) www.interpol.int

Международная электротехническая комиссия www.iec.ch

Международная организация по стандартизации www.iso.org

7.4. Целевая группа по осуществлению контртеррористических мероприятий (ЦГОКМ)

Секретариат Организации Объединенных Наций, ее фонды, учреждения и программы и связанные с ней организации способствуют осуществлению Глобальной контртеррористической стратегии Организации Объединенных Наций как посредством выполнения своих индивидуальных мандатов, так и в рамках своего членства в Целевой группе по осуществлению контртеррористических мероприятий.

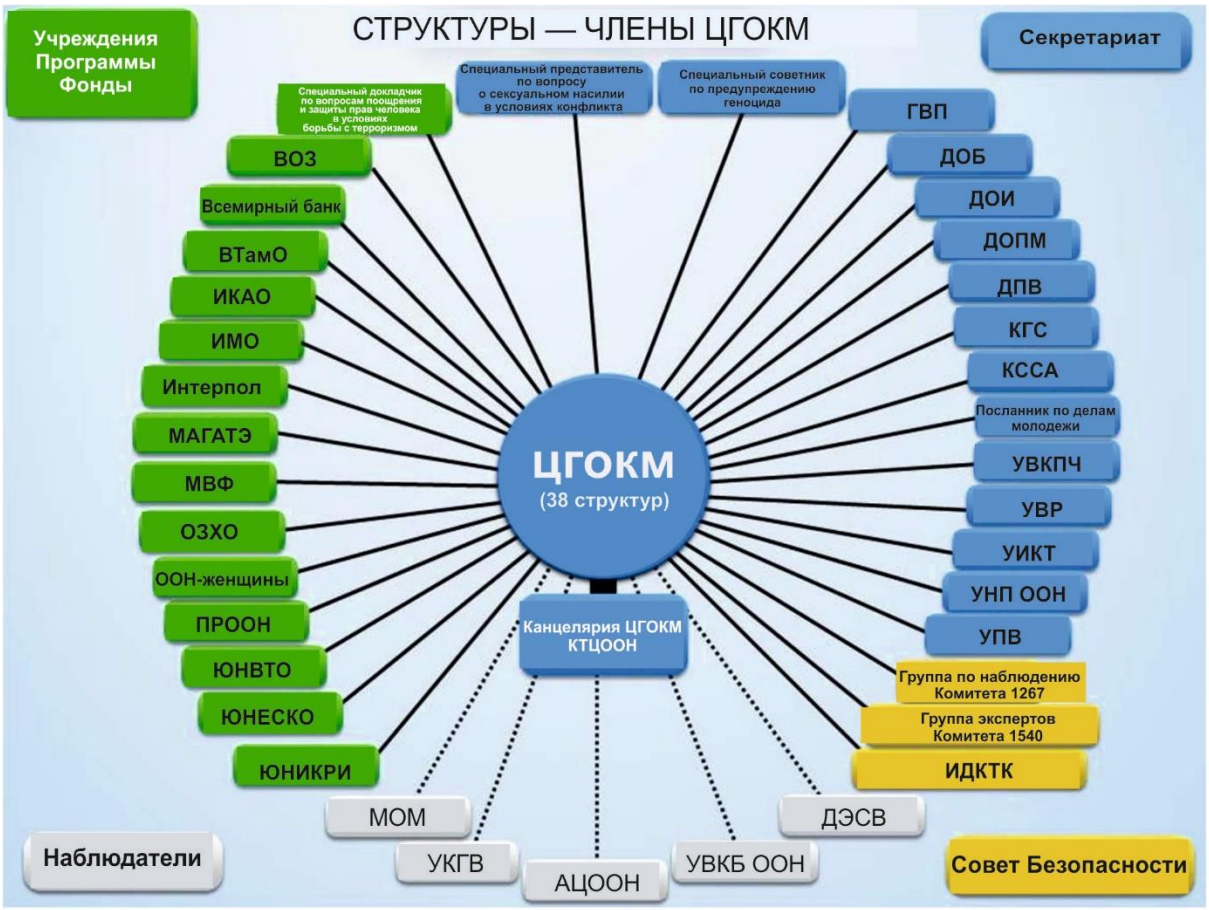
В состав Целевой группы входят 38 международных структур и Интерпол, которые в силу характера своей деятельности принимают участие в многосторонних усилиях по борьбе с терроризмом. Каждая структура вносит свой вклад в общую работу в соответствии со своим мандатом. Членами Целевой группы являются:

1. Всемирная организация здравоохранения (ВОЗ)
2. Всемирная таможенная организация (ВТамО)
3. Всемирная туристская организация (ЮНВТО)
4. Всемирный банк
5. Группа Организации Объединенных Наций по вопросам верховенства права
6. Группа по наблюдению за организацией «Аль-Каида» и движением «Талибан»
7. Группа экспертов Комитета 1540
8. Департамент общественной информации (ДОИ)
9. Департамент операций по поддержанию мира (ДОПМ)
10. Департамент по вопросам охраны и безопасности (ДОБ)
11. Департамент по политическим вопросам (ДПВ)

12. Исполнительный директорат Контртеррористического комитета (ИДКТК)
13. Канцелярия Генерального секретаря (КГС)
14. Канцелярия Специального посланника Генерального секретаря по делам молодежи
15. Канцелярия Специального представителя Генерального секретаря по вопросу о детях и вооруженных конфликтах (КСПГС-ДВК)
16. Канцелярия Специального советника Генерального секретаря по предупреждению геноцида
17. Канцелярия Специального советника Организации Объединенных Наций по Африке (КССА)
18. Международная морская организация (ИМО)
19. Международная организация гражданской авиации (ИКАО)
20. Международная организация уголовной полиции (Интерпол)
21. Международное агентство по атомной энергии (МАГАТЭ)
22. Международный валютный фонд (МВФ)
23. Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия (ЮНИКРИ)
24. ООН-женщины
25. Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО)
26. Организация по запрещению химического оружия (ОЗХО)
27. Программа развития Организации Объединенных Наций (ПРООН)
28. Специальный докладчик по вопросам поощрения и защиты прав человека в условиях борьбы с терроризмом
29. Управление Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ)
30. Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН)
31. Управление по вопросам разоружения (УВР)
32. Управление по правовым вопросам (УПВ)

Наблюдатели

33. Альянс цивилизаций Организации Объединенных Наций (АЦООН)
34. Департамент Организации Объединенных Наций по экономическим и социальным вопросам (ДЭСВ)
35. Международная организация по миграции (МОМ)
36. Управление Верховного комиссара Организации Объединенных Наций по делам беженцев (УВКБ ООН)
37. Управление по координации гуманитарных вопросов (УКГВ)



Рабочая группа ЦГОКМ по вопросам управления границами и правоохранительной деятельности в контексте борьбы с терроризмом

Данная Рабочая группа была создана в целях предоставления государствам-членам рекомендаций в отношении осуществления необходимых правовых, институциональных и практических мер пограничного контроля в связи с борьбой с терроризмом. Рабочая группа уделяет основное внимание следующим областям: передвижения террористов; надежность и защищенность документов на въезд/выезд; незаконное перемещение денежной наличности и оборотных кредитно-денежных документов на предъявителя; перемещение и обработка товаров; незаконное перемещение стрелкового оружия, легких вооружений, боеприпасов, взрывчатых веществ и оружия массового уничтожения; авиационная безопасность и безопасность на море; системы раннего предупреждения и оповещения; и контроль за открытыми границами.

Мандат

Рабочая группа была создана в целях оказания государствам-членам помощи в укреплении их систем управления границами и пограничного контроля, как это предусмотрено в пунктах 4, 5, 7, 8 и 13–16 раздела II и пунктах 2, 4 и 11–13 раздела III Глобальной контртеррористической стратегии Организации Объединенных Наций (A/RES/60/288).

Разработан круг ведения Рабочей группы по вопросам управления границами в контексте борьбы с терроризмом.

Текущее состояние

В настоящее время Рабочая группа занимается осуществлением проекта координированного управления границами и компилированием всех соответствующих международных конвенций, стандартов и практических рекомендаций в простом и удобном для пользования формате в целях оказания государствам-членам помощи в укреплении институциональных и процедурных механизмов в рамках

эффективной системы управления границами. Рабочая группа завершила создание рабочей модели координированного управления границами. Эта модель будет совершенствоваться за счет постоянного диалога и консультаций с государствами-членами и международными организациями.

Структуры

Сопредседатели

- Исполнительный директорат Контртеррористического комитета (ИДКТК) (ведущий)
- Всемирная таможенная организация (ВТамО)
- Международная организация уголовной полиции (Интерпол)

Основные структуры
Канцелярия ЦГОКМ

- Международная организация гражданской авиации (ИКАО)
- Международная морская организация (ИМО)
- Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН)
- Международная организация по миграции (МОМ)
- Управление Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ)
- Международный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия (ЮНИКРИ)
- Управление по вопросам разоружения (УВР)
- Группа экспертов Комитета 1540
- Группа по наблюдению Комитета 1267
- Управление Верховного комиссара Организации Объединенных Наций по делам беженцев (УВКБ ООН) (наблюдатель)

Другие участвующие структуры-члены

- Департамент операций по поддержанию мира (ДОПМ)
- Организация по запрещению химического оружия (ОЗХО)
- Программа развития Организации Объединенных Наций (ПРООН)
- Всемирная организация здравоохранения (ВОЗ)
- Департамент по экономическим и социальным вопросам (ДЭСВ)

Рабочая группа осуществляет свою деятельность по следующим основным тематическим направлениям:

- Перемещение лиц и обработка их данных
- Надежность и защищенность процедуры выдачи документов
- Перемещение денежной наличности и оборотных документов на предъявителя
- Перемещение и обработка товаров
- Перемещение стрелкового оружия, легких вооружений, боеприпасов, взрывчатых веществ и химических, биологических, радиоактивных и ядерных материалов
- Безопасность на море
- Авиационная безопасность
- Системы раннего предупреждения и оповещения
- Контроль за открытыми границами
- Настоятельная необходимость в обеспечении соблюдения прав человека

Перемещение лиц и обработка их данных

Одним из важных последствий террористических нападений, совершавшихся в последние годы по всему миру, является обеспечение более четкой связи между перемещением лиц через границы и принятием мер по обеспечению национальной безопасности. Поскольку сами процессы, которые призваны содействовать организации поездок и осуществлению экономических и культурных обменов, используются в том числе и террористами, меры, направленные на предотвращение терроризма, становятся неразрывно связанными с управлением и регулированием трансграничных перемещений. Эти меры предусматривают внедрение комплексных систем управления границами, предназначенных для обслуживания пассажиров, выдачу защищенных проездных документов, содействие обмену информацией между заинтересованными сторонами, подготовку кадров и укрепление потенциала. Позитивные изменения в этих областях могут способствовать совершенствованию систем безопасности и иммиграционных механизмов, содействуя в то же время трансграничному перемещению лиц. Некоторые из этих мер являются технологически сложными и в высшей степени инновационными, однако некоторые более простые меры могут применяться в традиционных сферах управления миграционными потоками в целях укрепления общего потенциала. В любом случае использование таких мер должно обосновываться степенью ожидаемой угрозы, особенно с учетом того, что усиление мер безопасности может привести к созданию дополнительных помех и потенциальному вторжению в частную жизнь и посягательству на гражданские права.

Надежность и защищенность процедуры выдачи документов

Важными инструментами предотвращения передвижения террористов и борьбы с трансграничной преступностью являются системы обеспечения защищенности проездных документов и идентификации. В руках террористов подложный проездной документ может оказаться таким же опасным, как и оружие. Поскольку современные паспорта становятся все более защищенными и подделывать их становится все труднее, уголовные преступники и террористы все чаще пытаются фальсифицировать вспомогательные документы (свидетельства о рождении, национальные удостоверения личности и т.д.) либо ходатайствовать о получении «официально выдаваемых» паспортов. Поэтому для устранения этих факторов уязвимости государствам необходимо разработать и внедрить универсальные спецификации для управления идентификационной информацией и обеспечения защищенности проездных документов (включая процедуру выдачи).

Перемещение денежной наличности и оборотных документов на предъявителя

Контрабанда денежной наличности и/или оборотных документов на предъявителя (ОДП) через границы является одним из предпочитаемых террористами методов перемещения средств через международные границы для целей либо финансирования террористической деятельности, либо отмывания доходов от незаконной деятельности. В целях выявления и предотвращения незаконного перемещения денежной наличности и ОДП правительства поручают своим таможенным службам осуществлять меры пограничного контроля, отвечающие международным нормам. Строгое соблюдение этих норм позволит повысить эффективность мер пограничного контроля в этой области. Борьба с финансированием террористической деятельности является неотъемлемой частью подхода, используемого Организацией Объединенных Наций в борьбе с терроризмом, что нашло отражение во многих ее резолюциях и конвенциях.

Перемещение и обработка товаров

Особенно подвержены манипулированию со стороны террористов мировая торговля и международная система поставок. В целях сведения этого фактора уязвимости до минимума необходимо принять ряд мер, включая обеспечение получения предварительной электронной информации о ввозимых, вывозимых и транзитных грузах; применение последовательного подхода к управлению рисками в целях устранения угроз безопасности грузов; использование неинтрузивной аппаратуры обнаружения; содействие сотрудничеству между таможенными управлениями (например, посредством проведения досмотра особо опасных вывозимых контейнеров и грузов); и налаживание партнерских отношений с частным сектором в целях использования защищенных процедур на каждом этапе

функционирования цепочки поставок в рамках программ «уполномоченных экономических операторов» (УЭО). Осуществление этих и связанных с ними мер имеет важное значение для повышения безопасности международной торговли и содействия перемещению товаров через международные границы.

Перемещение стрелкового оружия, легких вооружений, боеприпасов, взрывчатых веществ и химических, биологических, радиоактивных и ядерных материалов

Незаконный оборот и перемещение стрелкового оружия, легких вооружений, обычных боеприпасов и взрывчатых веществ, а также химических, биологических, радиоактивных и ядерных материалов и товаров двойного назначения в сочетании с изменением структуры торговли оружием и вовлечением неторговых субъектов представляют собой серьезные проблемы, которые необходимо решать в рамках глобальных усилий по борьбе с терроризмом. В руках террористов эти боеприпасы и материалы становятся компонентами террористических нападений. Свести к минимуму опасность того, что такие товары будут либо перенаправлены, либо незаконным путем приобретены негосударственными субъектами, можно с помощью эффективного регулирования, экспортного контроля и управления границами, включая принятие законодательных и правоприменительных мер. Такие меры должны учитывать необходимость поддержания надлежащего баланса между экспортным контролем и содействием развитию законной торговли.

Безопасность на море

Свыше 90% всех товаров, торговля которыми осуществляется на международном уровне, перевозятся из мест происхождения в места назначения по основным мировым морским торговым путям. Поэтому безопасность на море является вопросом, имеющим общемировое значение. Цели обеспечения безопасности на море заключаются в том, чтобы выявлять угрозы безопасности и противодействовать им; принимать меры по предотвращению инцидентов, затрагивающих безопасность судов или портовых сооружений; и обеспечивать безопасность пассажиров, экипажей, судов и их грузов, портовых сооружений и лиц, которые работают в портах и проживают вблизи них, и в то же время предоставлять возможности для безопасного и эффективного ведения морской торговли. Для предотвращения противоправных деяний в отношении пассажиров и экипажей судов, осуществляющих международные рейсы, и в отношении портовых сооружений, которые обслуживают их, необходимо эффективное осуществление соответствующих законодательных мер и практических мер по обеспечению безопасности.

Авиационная безопасность

Акты терроризма по-прежнему представляют серьезные и постоянные угрозы для международной гражданской авиации. Борьба с такими угрозами требует разработки всеобъемлющих и надежных стратегий и мер безопасности, направленных на обеспечение физической безопасности воздушных судов и аэропортов. Принятие законодательных положений, предусматривающих уголовное наказание за акты незаконного вмешательства в деятельность гражданской авиации, и эффективное осуществление и обеспечение соблюдения соответствующих стандартов и процедур авиационной безопасности позволят государствам значительно расширить свои возможности по защите от таких угроз.

Системы раннего предупреждения и оповещения

Обеспечение безопасности границ представляет собой динамичный и совершенствующийся процесс. Поскольку незаконное трансграничное перемещение лиц негативно сказывается не только на безопасности, но и на политическом, экономическом и социальном благополучии государств, правительства уделяют сейчас основное внимание совместным усилиям по обеспечению безопасности, понимая, что односторонние действия уже не являются эффективными. Поэтому ключевыми компонентами эффективных систем управления границами являются комплексные системы раннего предупреждения и оповещения. Они позволяют укрепить коллективный потенциал государств в плане выявления и предотвращения актов терроризма и борьбы с ними посредством содействия развитию

межведомственного сотрудничества и своевременного предоставления соответствующей надежной информации и обмена ею, что способствует ответственному принятию важнейших решений.

Многие международные организации, мандат которых охватывает вопросы пограничного контроля, применяют системы раннего предупреждения и оповещения или способствуют их внедрению с использованием инструментов, разработанных какой-либо отдельной организацией, либо инструментов, разработанных для применения международным сообществом. К числу этих инструментов относятся сети Всемирной таможенной организации (ВТамО) CEN и RILO; системы Международной морской организации (ИМО) SOLAS, LRIT и AIS; сводные перечни комитетов по санкциям Совета Безопасности и защищенная глобальная система связи «I-24/7», база данных об украденных или утерянных проездных документах и режим уведомлений Международной организации уголовной полиции (Интерпол).

Контроль за открытыми границами

Режим открытой границы (полоса между официальной сухопутной границей и контрольно-пропускными пунктами морского порта) по-прежнему способствует незаконному трансграничному перемещению лиц, в том числе террористов и уголовных преступников, и товаров (включая стрелковое оружие, легкие вооружения, боеприпасы, взрывчатые вещества и химические, биологические, радиоактивные и ядерные материалы). Правительства признают важность обеспечения безопасности открытых границ и в этих целях принимают различные меры, включая наблюдение, патрулирование, установку физических барьеров, проведение совместных операций по обеспечению контроля и патрулированию, обмен информацией, анализ оперативных данных и взаимодействие с приграничным населением в вопросах контроля и охраны порядка. Для эффективного устранения рисков, связанных с режимом открытой границы, необходимо, чтобы соответствующие органы власти предпринимали согласованные усилия по обеспечению контроля.

Настоятельная необходимость в обеспечении соблюдения прав человека

В Глобальной контртеррористической стратегии Организации Объединенных Наций находит отражение твердая убежденность государств-членов в том, что эффективные меры борьбы с терроризмом и защита прав человека не противоречат друг другу, а представляют собой дополняющие и подкрепляющие друг друга цели и что права человека и верховенство права являются фундаментальной основой глобальных усилий по борьбе с терроризмом. Принимая Глобальную стратегию и содержащийся в ней План действий, государства-члены постановили «признать, что международное сотрудничество и любые меры, которые мы примем для предотвращения терроризма и борьбы с ним, должны обеспечивать соблюдение всех наших обязательств по международному праву, в том числе по Уставу Организации Объединенных Наций и соответствующим международным конвенциям и протоколам, в частности норм в области прав человека, беженского права и международного гуманитарного права» (A/RES/60/288, приложение, пункт 3 преамбулы; вновь подтверждено в A/RES/64/297). Генеральная Ассамблея также подчеркнула настоятельную необходимость в обеспечении соблюдения прав человека в рамках усилий по борьбе с терроризмом в более чем 60 резолюциях о международном терроризме. Что касается, в частности, пограничного контроля, то Ассамблея призвала государства «принять меры к тому, чтобы все инструкции, касающиеся работы служб пограничного контроля и других механизмов, действующих до въезда в страну, и соответствующие процедуры были ясными и четкими и обеспечивали полное соблюдение их обязательств по международному праву, и в частности по международному беженскому праву и международному праву в области прав человека, в отношении лиц, ищущих международной защиты» (A/RES/62/159, пункт 8 постановляющей части; вновь подтверждено в A/RES/64/221).