

A banner for the 'ID@Borders & Future of Travel Conference 2019' held in Vienna, Austria. The banner features a blurred image of people walking in a hallway, overlaid with a red semi-transparent bar containing the conference title and dates.

ID@Borders & Future of Travel Conference 2019
11-12 APRIL 2019 HOFBURG, VIENNA, AUSTRIA

ИТОГОВЫЙ ДОКУМЕНТ

Организовано
Организацией по безопасности и сотрудничеству в Европе
совместно с Институтом биометрии

Вена, 11-12 апреля 2019 года

1. Резолюция Совета Безопасности ООН 2396:

В последние годы угроза, исходящая от иностранных боевиков-террористов (ИБТ), стала предметом серьезной международной озабоченности. **Увеличение числа ИБТ, возвращающихся** в страны происхождения и прежнего проживания или перемещающихся в третьи страны, **создает опасность**, что их боевой опыт будет использован для планирования и осуществления нападений, создания новых террористических ячеек или будет иным образом способствовать совершению **террористических актов в будущем**. Именно поэтому в декабре 2017 года Совет Безопасности ООН принял [резолюцию 2396](#), ставшую важной вехой в международных усилиях по выявлению и пресечению перемещений ИБТ, особенно тех, кто возвращается или переезжает из зон конфликтов.



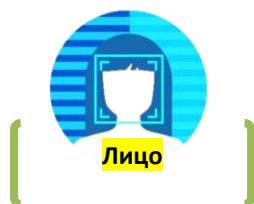
2396 создает
новые
обязательства в
отношении
биометрии и
безопасности
границ

1. Постановляет, что государства-члены должны 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 иностранных боевиков-террористов, в соответствии с внутренним законодательством и нормами международного права в области прав человека.
2. Рекомендует государствам-членам **делиться этими данными**, сообразно обстоятельствам, с соответствующими государствами-членами, а также с **Интерполом** и другими соответствующими международными органами.
3. Призывает государства-члены, международные, региональные и субрегиональные организации **предоставлять** государствам-членам **техническую помощь, ресурсы и поддержку в наращивании потенциала** для применения таких систем.

Основная ответственность в борьбе с терроризмом лежит на государствах, однако международные и региональные организации могут и должны играть вспомогательную роль и оказывать поддержку государствам, реагирующим на эти трансграничные угрозы. Именно поэтому [ОБСЕ](#) объединилась с [Институтом биометрии](#) и совместно организовала 11-12 апреля 2019 года в Вене конференцию [«Установление личности на границе и будущее путешествий»](#). Цель конференции заключалась в (а) **повышении осведомленности** о преимуществах использования биометрических технологий на границе и ответственного использования этих данных в борьбе с терроризмом; и (б) **поощрении передового опыта** в области обмена биометрическими данными.



2. Что такое биометрия?



БИОМЕТРИЯ – ЭТО БИОЛОГИЧЕСКИЕ И ПОВЕДЕНЧЕСКИЕ ХАРАКТЕРИСТИКИ ИНДИВИДА, КОТОРЫЕ МОГУТ БЫТЬ ВЫДЕЛЕНА В КАЧЕСТВЕ ОТЛИЧИТЕЛЬНЫХ, ПОВТОРЯЮЩИХСЯ БИОМЕТРИЧЕСКИХ ПРИЗНАКОВ ДЛЯ БИОМЕТРИЧЕСКОГО РАСПОЗНАВАНИЯ ИНДИВИДОВ.

Общие признаки биометрических методов измерений

УНИВЕРСАЛЬНЫЕ

УНИКАЛЬНЫЕ

НЕИЗМЕННЫЕ

ИЗМЕРИМЫЕ

ЭФФЕКТИВНЫЕ

СОЦИАЛЬНО
ПРИЕМЛЕМЫЕ

Стандартная биометрическая операционная модель

Биометрические системы идентификации по существу являются системами распознавания образов. Они используют сканирующие устройства и камеры для получения изображений или измерений индивидуальных характеристик, а также компьютерное оборудование и программное обеспечение для извлечения, кодирования, хранения и сравнения этих характеристик. Обычно этот процесс полностью автоматизирован, что позволяет принимать решения очень быстро, в большинстве случаев всего за несколько секунд. Стандартная операционная модель базовой биометрической системы состоит из следующих этапов:

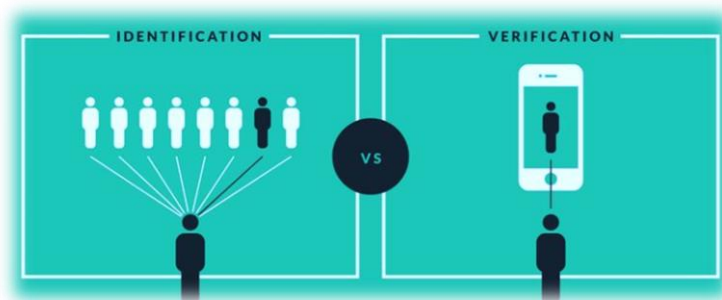
- ✚ **Приобретение и регистрация** – получение биометрического образца индивида с помощью устройства для сбора данных
- ✚ **Извлечение данных** – преобразование полученных биометрических образцов в биометрические шаблоны
- ✚ **Хранение данных** – хранение зарегистрированных данных в системе или базе данных
- ✚ **Сравнение данных** – доступ к базе данных и получение одного или нескольких ранее зарегистрированных шаблонов для сравнения с представленным шаблоном
- ✚ **Совпадение данных** – использование алгоритмов для определения, соответствует ли шаблон запроса выбранным шаблонам базы данных
- ✚ **Получение результата** – ‘совпадение’ ИЛИ ‘несовпадение’



3. Биометрические системы

сопоставления:

Работа всех биометрических систем начинается с процесса регистрации, за которым следует процесс сопоставления, использующий **верификацию** и/или **идентификацию**.



(1) **Верификация** («один к одному» или 1:1) – эта модель использует подтвержденную личность для выбора из базы данных или электронного документа только одного шаблона и сопоставления его с *исследуемым шаблоном*.

В процессе верификации задается вопрос:



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

(2) **Идентификация** («один ко многим» или 1:n) – эта поисковая функция не нуждается в подтвержденной личности. *Шаблон запроса* просматривает всю базу данных в поисках потенциального совпадения.

Идентификация задает вопрос:



«Внесены ли вы в базу данных, и если да, то какой записи вы соответствуете?»



Эффективные биометрические системы объединяют задачи верификации и идентификации для повышения надежности идентификации личности и сравнения со справочными наборами данных.



Электронные ворота: пример биометрической системы на границе

Электронные ворота работают в нескольких аэропортах региона ОБСЕ. При прохождении этих ворот сканируется электронный паспорт, и биометрическая информация, содержащаяся в чипе паспорта, сравнивается при помощи технологии распознавания лиц со сканом лица путешественника. Другими словами, электронные ворота выполняют процесс верификации. Их можно также подключить к контрольным спискам, таким как глобальные базы данных Интерпола, и сравнить биометрическое изображение путешественника со справочными базами данных лиц, вызывающих озабоченность. В этом случае электронные ворота осуществляют процесс идентификации. Исходя из зарегистрированных и удостоверенных биометрических данных, личность путешественника подтверждается на границе в процессе верификации, однако поиск по биометрическому контрольному списку может выявить, что подтвержденная личность представляет особый интерес.

4. Последствия для конфиденциальности данных, связанные с биометрией

Резолюция СБ ООН 2386 четко указывает, что государства должны собирать биометрические данные в соответствии с внутренним законодательством и нормами международного права в области прав человека. [«Сборник практических рекомендаций ООН по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом»](#) предусматривает следующее:

Обработка данных	Государства должны назначить контролера данных, который будет отвечать за руководство всеми мероприятиями по обработке данных.
Обмен данными	Обмен данными должен подчиняться национальному законодательству и регламентироваться четкой нормативно-правовой базой. Обмен данными должен осуществляться только с заслуживающими доверия получателями и в целях, установленных законом.
Предотвращение противоправного использования данных	Государства должны обеспечить защиту всех биометрических данных от несанкционированного доступа и противоправного использования, а также обеспечить точность предоставляемых данных и гарантировать, что эти данные предоставляются не в злонамеренных целях.
Надзор	Для предотвращения произвольного сбора и хранения биометрических данных необходимо создать эффективные и беспристрастные механизмы надзора со стороны независимого органа, к которому отдельные лица могли бы иметь доступ.

5. Преимущества биометрии в условиях борьбы с терроризмом

Комплексные стратегии пограничного контроля играют важнейшую роль в борьбе с терроризмом в целом и иностранными боевиками-террористами в частности. Именно поэтому биометрические системы и базы данных широко используются в правоохранительной деятельности, обеспечении пограничного режима и военных целях. Государства также рассматривают преимущества **обмена биометрическими данными в двустороннем, многостороннем, региональном и глобальном масштабе в контексте международных прав человека.**



Биометрические данные, используемые совместно с другими разведывательными данными, могут использоваться упреждающим образом для предотвращения террористических актов. Биометрические справочные данные или данные с места преступления могут использоваться для доказательства или опровержения причастности лица к преступлению, а также установления связи лица с деятельностью, событием, местом или другим лицом *до, во время или после инцидента.*

IMPORTANT

- ✓ Помните об **угрозах и уязвимостях**, возникающих в результате изменения некоторых биометрических модальностей. Более подробную информацию см. на стр. 36-39 [«Сборника практических рекомендаций ООН по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом»](#).
- ✓ Уважайте принцип **конфиденциальности данных** в соответствии с международными правовыми стандартами. Более подробную информацию вы найдете на стр. 25-35 Сборника ООН, а также в:
 - Публикациях Агентства фундаментальных прав ЕС ([EU FRA](#)): [«Под бдительным присмотром: биометрия, системы ИКТ ЕС и основные права»](#), [«Хранение биометрических данных в документах, удостоверяющих личность, и видах на жительство, и его значение для основных прав»](#).
 - И публикациях [правозащитного учреждения ОБСЕ](#): [«Руководящие принципы противодействия угрозам и вызовам со стороны "иностраных боевиков-террористов" в контексте прав человека»](#).



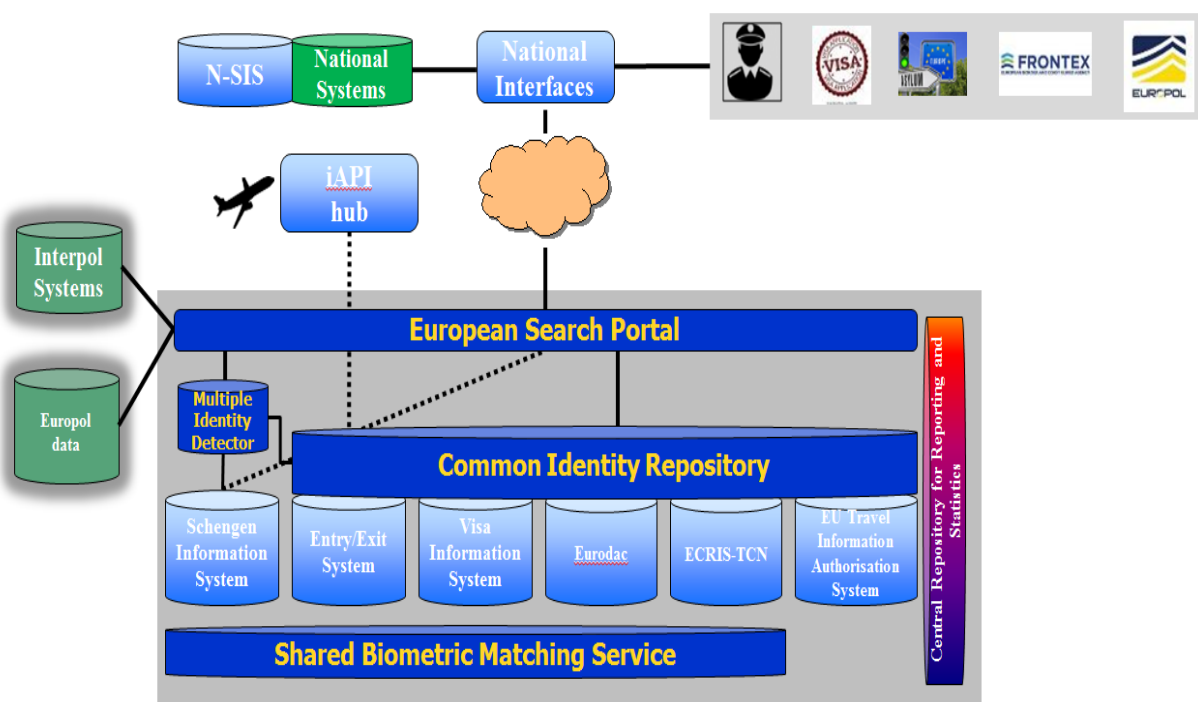
6. Обновленная информация от ЕС и Интерпола



В феврале 2019 года Европейский парламент и Совет достигли предварительного политического соглашения о создании основы для оперативной совместимости информационных систем ЕС в области безопасности, миграции и пограничного режима. Цель этой работы - предоставление сотрудникам пограничной службы и полиции доступа к правильной информации.

Новые компоненты позволят существующим и будущим информационным системам ЕС, таким как система въезда/выезда (EES) и Европейская система информации и авторизации путешественников (ETIAS), взаимодействовать друг с другом, предотвращая тем самым потерю важных элементов информации. Новые инструменты позволят:

- ✚ **Проверить имеющиеся данные одним щелчком мыши:** Европейский поисковый портал позволит сотрудникам пограничной службы и полиции проводить одновременную проверку документов, удостоверяющих личность, во всех информационных системах ЕС на одном экране;
- ✚ **Лучше выявлять случаи мошенничества с использованием личных данных:** общее хранилище личных данных, в котором будут храниться биографические данные лиц, не являющихся гражданами ЕС, позволит сотрудникам пограничной службы и полиции лучше выявлять опасных преступников;
- ✚ **Улучшить доступ для правоохранительных органов:** как только информация, запрашиваемая сотрудником, будет соответствовать информации, содержащейся в одной из систем (т.е. получит "совпадение"), он/она сможет запросить более целенаправленный доступ, в соответствии с конкретными правилами для каждой системы;
- ✚ **Защитить основные права:** правила доступа и ограничения по назначению информационных систем ЕС не изменятся, обеспечивая тем самым защиту основных прав.



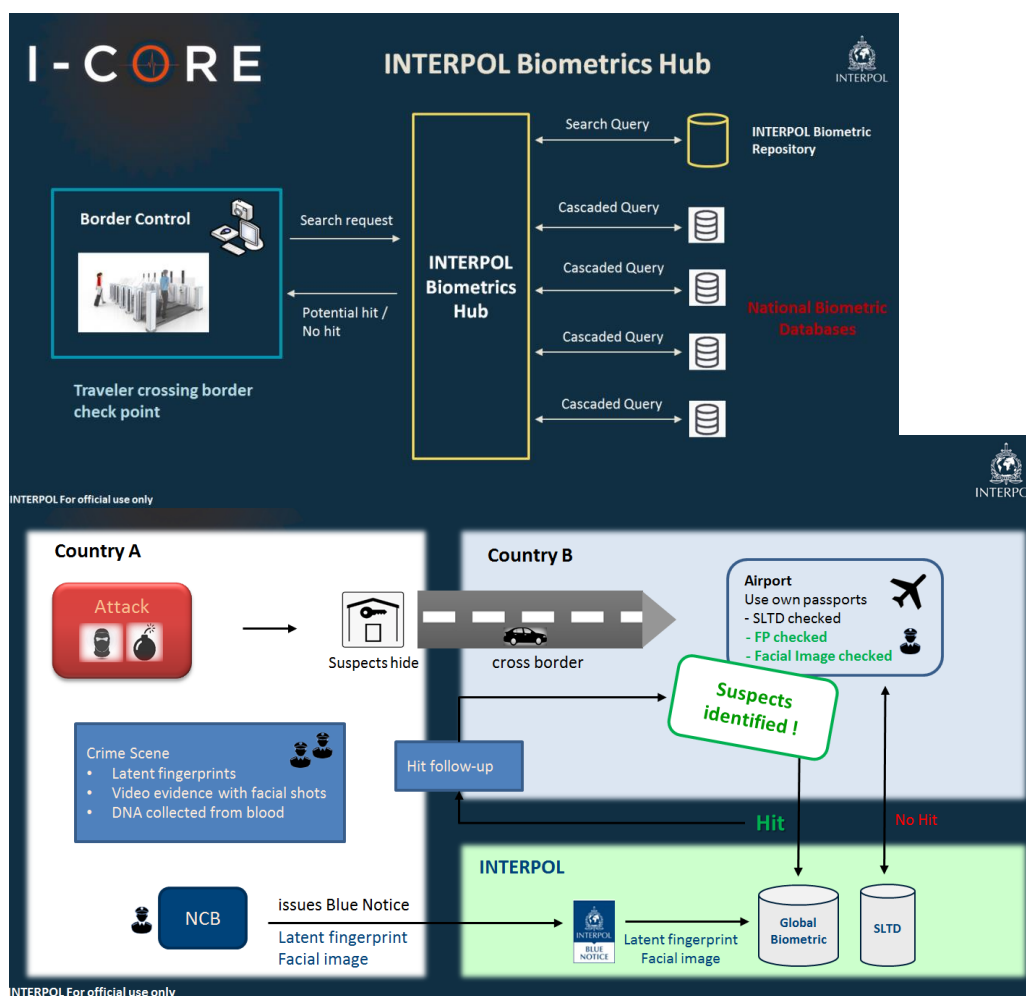


Интерпол обладает уголовными **базами данных отпечатков пальцев, профилей ДНК и изображений лиц**, предоставленных странами-членами. Это позволяет полиции во всем мире устанавливать связи между преступниками и местами преступлений. Интерпол также обучает оперативных сотрудников методам оценки, хранения и обмена доказательствами в соответствии с передовой практикой.

Уполномоченные пользователи в странах-членах могут просматривать, представлять и перепроверять записи в базе данных отпечатков пальцев через удобную для пользователя **Автоматическую систему идентификации отпечатков пальцев (AFIS)**.

База данных ДНК содержит профили ДНК преступников, пропавших без вести лиц, неопознанных тел, а также ДНК, полученные на месте преступления. Интерпол не хранит никаких номинальных данных, связывающих профиль ДНК с каким-либо лицом. **База данных Системы распознавания лиц** является специальной платформой для хранения и перекрестной проверки изображений в целях идентификации лиц, скрывающихся от правосудия, пропавших без вести и представляющих особый интерес.

В настоящее время Интерпол проводит исследование об использовании биометрических данных для выявления лиц, представляющих особый интерес (террористов, известных преступников), на пограничном контроле и планирует создать **центр биометрических данных** (защищенный шлюз) для связи биометрических баз данных стран-членов с биометрическими базами данных Интерпола – это модель, основанная на общих данных.



7. Примеры передового опыта государств - участников ОБСЕ:

КАНАДА: Биометрическая информация является основополагающим инструментом для поддержки программы модернизации канадского правительства. Точное определение личности лежит в основе всех иммиграционных решений:

- необходимо как можно раньше получить правильную идентичность, связав человека (биометрические данные) с ключевыми признаками (биографическими);
- если невозможно зафиксировать личность, правительство не может быть уверено в том, что последующая проверка на соответствие критериям приемлемости и допустимости может привести к значимым результатам.

В 2018 году Канада расширила сбор биометрических данных:

- все иностранные граждане (кроме освобожденных), ходатайствующие о временном или постоянном виде на жительство, обязаны сдать отпечатки пальцев и предоставить фотографию.

Следующие шаги в использовании биометрических данных в Канаде:

- Переход на верификационную модель;
- Создание новых международных механизмов обмена информацией;
- Сбор биометрических данных у других категорий заявителей.



СОЕДИНЕННЫЕ ШТАТЫ: Национальная передовая технология распознавания (HART) - это современная биометрическая система, которая дополняет Автоматизированную систему биометрической идентификации (IDENT), находящуюся в ведении Управления биометрической идентификации (OBIM) Министерства национальной безопасности США.

Система HART внедрила новые услуги и технологические достижения: *повышение эффективности и доступности; расширенная функциональная совместимость; повышенная конфиденциальность и безопасность ИКТ; новый дизайн с экономичностью; повышенная точность и подтверждение идентификации; увеличение пропускной способности.*

В 2018 финансовом году OBIM:

- Обработала ~113 миллионов субъектов
- Выявила ~120,000 известных или подозреваемых террористов
- Выявила ~4.5 миллионов лиц с компрометирующей информацией

По мере появления новых оперативных задач и развития технологий HART сможет расти и адаптироваться для удовлетворения потребностей миссии. Для достижения этой цели необходимы новаторские решения в партнерстве с промышленностью и научными кругами.



8. Путь вперед: дальнейшие шаги ОБСЕ

Департамент по противодействию транснациональным угрозам ОБСЕ работает над проектом по оказанию помощи запрашивающим государствам - участникам ОБСЕ в сборе биометрических данных и обмене ими, как это предусмотрено резолюцией 2396 Совета Безопасности ООН. Проект будет состоять из трех основных этапов:



1 - Субрегиональные семинары по повышению осведомленности в Центральной Азии, Юго-Восточной Европе и Восточной Европе



2 - Национальные консультации для определения потребностей и целей



3 - Техническая поддержка, направленная на оказание помощи государствам при выявлении, приобретении и использовании биометрической системы, наилучшим образом отвечающей их потребностям

Вся работа будет осуществляться в тесном сотрудничестве и взаимодействии с *Институтом биометрии, Контртеррористическим управлением ООН и Интерполом.*



Для получения дополнительной информации, пожалуйста, свяжитесь с нами в ОБСЕ:

Simon Deignan simon.deignan@osce.org и Magda Jugheli magda.jugheli@osce.org