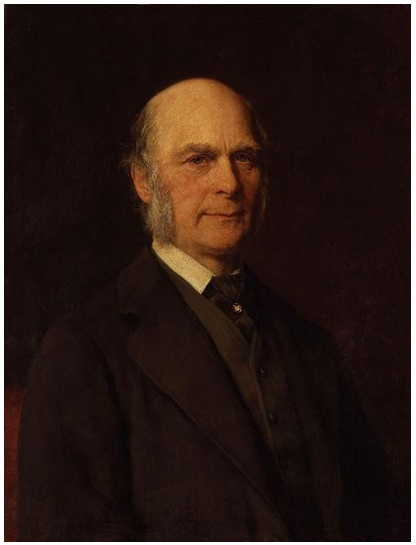
История возникновения и развития

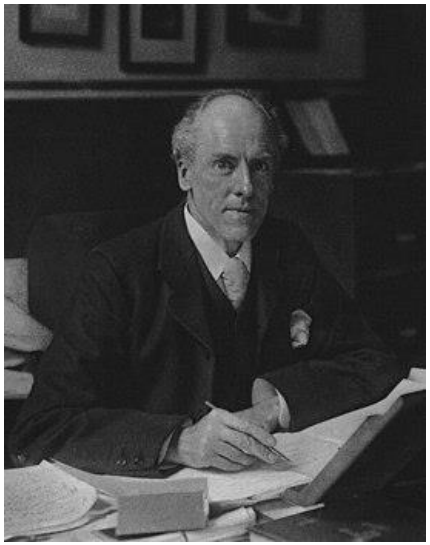
Биометрическая идентификация личности базируются на достижениях *бионики* (от греч. Bion — элемент жизни, буквально — живущий) — пограничной между биологией и техникой области науки, и изучает методы измерения физических характеристик и поведенческих черт человека для последующей идентификации и аутентификации личности.

Бионика тесно связана с биологией, физикой, химией, кибернетикой и инженерными науками — электроникой, навигацией, связью, морским делом и др.

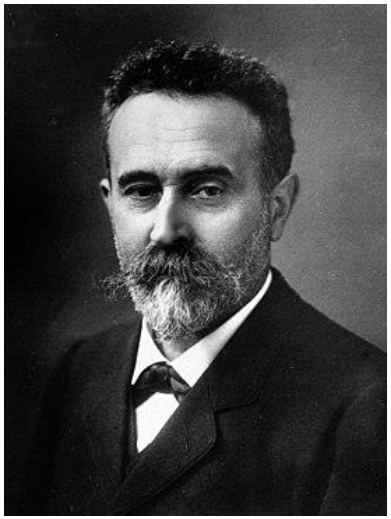
Прикладная бионика — наука, которая сочетает в себе биологию и технику.

В конце XIX в. *Ф. Гальтон* и *К. Пирсон*, изучая закономерности в наследственности людей, применили методы вариационной статистики к анализу различных особей и положили начало науке *биометрии*.

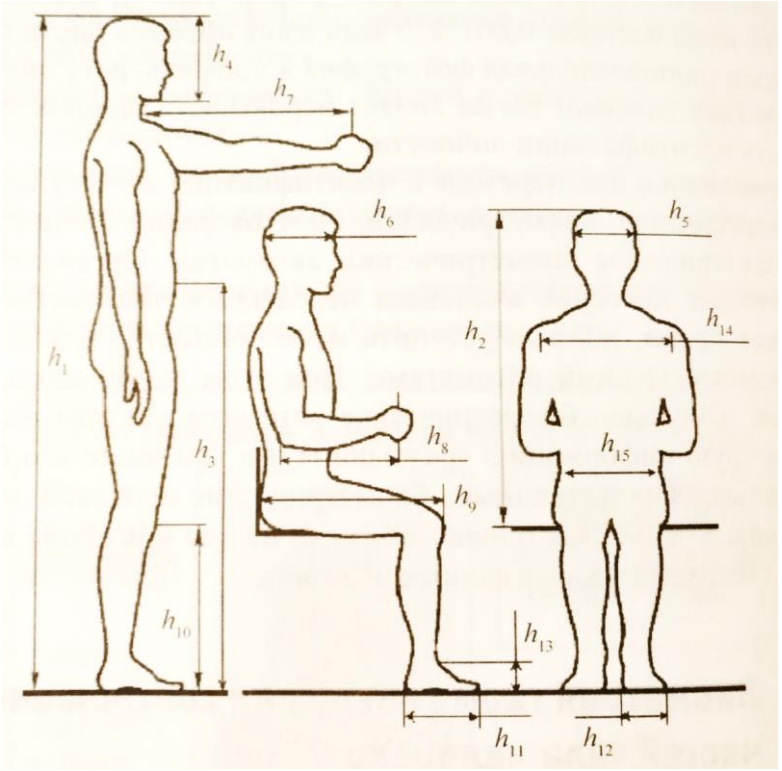




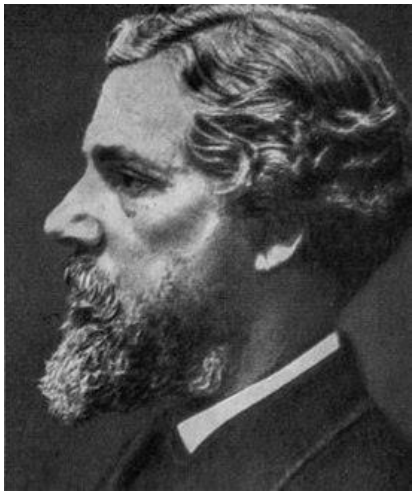
Особенности строения человеческого тела, лежащие в основе первых биометрических доктрин, внесли огромный вклад в развитие криминалистики. В конце XIX века для идентификации преступников в Европе использовалась процедура *бертильонажа*.



А. Бертильон в 1879 г. предложил для регистрации преступников использовать систему идентификации по практически неподверженным изменениям со временем антропометрическим измерениям: длина тела, длина каждой руки, словесный портрет, фото в анфас и профиль, описание особых примет преступника.



Дактилоскопия — способ опознания (идентификации) человека по следам пальцев рук (в том числе ладоней рук), основанный на неповторимости рисунка папиллярных линий кожи.



Основана на идеях У. Гершеля, выдвинувшего в 1877 г. гипотезу о неизменности папиллярного рисунка ладонных поверхностей кожи человека.

В начале XX в. Э. Генри предложил способ, благодаря которому идентификация по отпечаткам занимала несколько минут.

АДИС - автоматизированная дактилоскопическая идентификационная система.

Биометрические технологиии – автоматические или автоматизированные методы распознавания личности человека по его биологическим характеристикам или проявлениям.

Основные применения:

- криминалистика и экспертиза (форензика)
- ИБ (СКУД, системы голосования и др.)

Для идентификации применяются различные *биометрические характеристики человека* (БХЧ).

БХЧ:

- *статические*, связанные с его физическими характеристиками, например, отпечатком пальца, радужной оболочкой глаза, формой уха, изображением лица (2D или 3D) и др.;
- *динамические* или поведенческие, связанные с особенностями выполнения человеком каких-либо действий, например, походка, руковписный или клавиатурный почерк, голос и др.

Главные тенденции внедрения биометрического контроля доступа в различных отраслях рынка:

• *государство*, быстро движется к решениям, которые используют сенсоры для считывания отпечатков пальцев, способные проверять подлинность водительского удостоверения, паспорта или другого удостоверения личности, а также личности, у которой документ находится;

• *корпорации*, в современной бизнес-среде биометрия облегчает защиту документов, требуя от пользователей аутентификации с помощью карты, пропуска или отпечатка пальца;

• *здравоохранение*, биометрия будет играть большую роль в больницах при регистрации больных, в управлении очередями посетителей, защите конфиденциальности информации пациентов, при осуществлении платежей и обеспечении раздачи лекарств без утечки наркотических препаратов, а также при решении других задач повседневной деятельности;

• *банки*, биометрия будет продолжать распространяться в банковской отрасли по всему миру для повышения качества обслуживания клиентов при одновременном повышении безопасности банкоматов и других объектов;

• *транспорт*, биометрические системы дадут интеграторам возможность помочь клиентам в транспортной отрасли увеличить как безопасность, так и прибыль;

• *розничная торговля*, интегрированные биометрические считыватели улучшат проверку личности владельцев карт, используемых в платежных системах и программах лояльности, увеличат их функциональность и эффективность контроля доступа;

• *высшее образование*, новые типы решений для обеспечения обучения и безопасности, контроля доступа в лаборатории и другие важны объекты, в которых проводят эксперименты с опасными химическими веществами или биологическими и радиоактивными материалами;

• *защита информации*, разработка систем биометрической идентификация и аутентификации в сфере информационной безопасности по двум направлениям: физическая защита объектов информатизации, при которой к системе обработки допускается только нужные сотрудники, и допуск к информационным ресурсам компьютера конкретного сотрудника.

Основы идентификации в задачах ИБ

Идентификация – определение имени (логин или номер).

Аутентификация – проверка пароля (ключ или отпечаток пальца).

Авторизация – предоставление доступа.

Администрирование – регистрация действий пользователя.

Идентификация (от лат. identifico — отождествлять) —процесс опознавания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку.
Под идентификацией понимают также присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов [ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»].

Биометрическая идентификация — это процесс поиска по базе данных биометрических регистраций, направленный на поиск и возврат идентификатора(ов) биометрического контрольного шаблона, связанного с одним индивидом [ГОСТ ISO/IEC 2382-37-2016].

С практической точки зрения процесс идентификации рассматривается как сравнение введенного в систему идентификационного признака (кода) с образцами кодов, хранящимися в памяти системы (поиск и сравнение одного со многими).

Стадии идентификации в биометрической системе:

• регистрация идентификатора — сведения о физиологической или поведенческой характеристике преобразуются в форму, доступную компьютерным технологиям, и вносятся в память биометрической системы;
• выделение — из вновь предъявленного идентификатора выделяются уникальные признаки, анализируемые системой;
• сравнение — сопоставляются сведения о вновь предъявленном и ранее зарегистрированном идентификаторе;
• решение — выносится заключение о том, совпадают или не совпадают вновь предъявленный идентификатор.

Аутентификация (от греч. αυθεντικ΄ος — реальный или подлинный) — это процесс опознавания субъекта или объекта путем сравнения введенных идентификационных данных с эталоном (образом), хранящимся в памяти системы для данного субъекта или объекта [ГОСТ Р 51 241-2008].
Действие, доказывающее или показывающее бесспорное происхождение или достоверность [ГОСТ ISO/IEC 2382-37-2016 «Информационные технологии. Словарь. Часть 37. Биометрия»).

С практической точки зрения процесс аутентификации рассматривается как предоставление доказательств, что вы на самом деле есть тот, кем идентифицировались (от слова authentic — истинный, подлинный), т. е. рассматривается как сравнение одного с одним.

Два вида биометрических систем аутентификации:
• унимодальные — те, которые используют только одну особенность человека;
• мультимодальные (мультибиометрические) — использующие комбинацию унимодальных.

Авторизация — это процедура предоставления субъекту определенных полномочий и ресурсов в данной системе (проверка о разрешении доступа к запрашиваемому ресурсу).

Авторизация устанавливает сферу действия субъекта и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены.

Авторизация — это предоставление лицу возможностей в соответствие с положенными ему правами или проверка наличия прав при попытке выполнить какое-либо действие. Например, авторизацией являются лицензии на осуществление определённой деятельности.

В компьютерных системах:

- под *идентификацией* понимают получение учетной записи (identity) по username или email;

- под *аутентификацией* понимают проверку знания пароля от этой учетной записи;

- под *авторизацией* понимают проверку роли в системе и решение о предоставлении доступа к запрошенной странице или ресурсу.


Протоколы аутентификации
Использующие пароли и коды
На основе многоразовых паролей
На основе динамических (одноразовых) паролей
На основе PIN-кодов
Строгая аутентификация на основе использования криптографических методов и средств
На основе симметричных алгоритмов шифрования
На основе несимметричных алгоритмов шифрования
На основе однонаправленных ключевых хеш-функций
На основе алгоритмов электронной цифровой подписи
Биометрическая аутентификация пользователей
По отпечаткам пальцев
По геометрической форме кисти руки
По форме и размерам лица
По особенностям голоса
По узору радужной оболочки и сетчатке глаз
По клавиатурному почерку
По стоматологической матрице ротовой полости