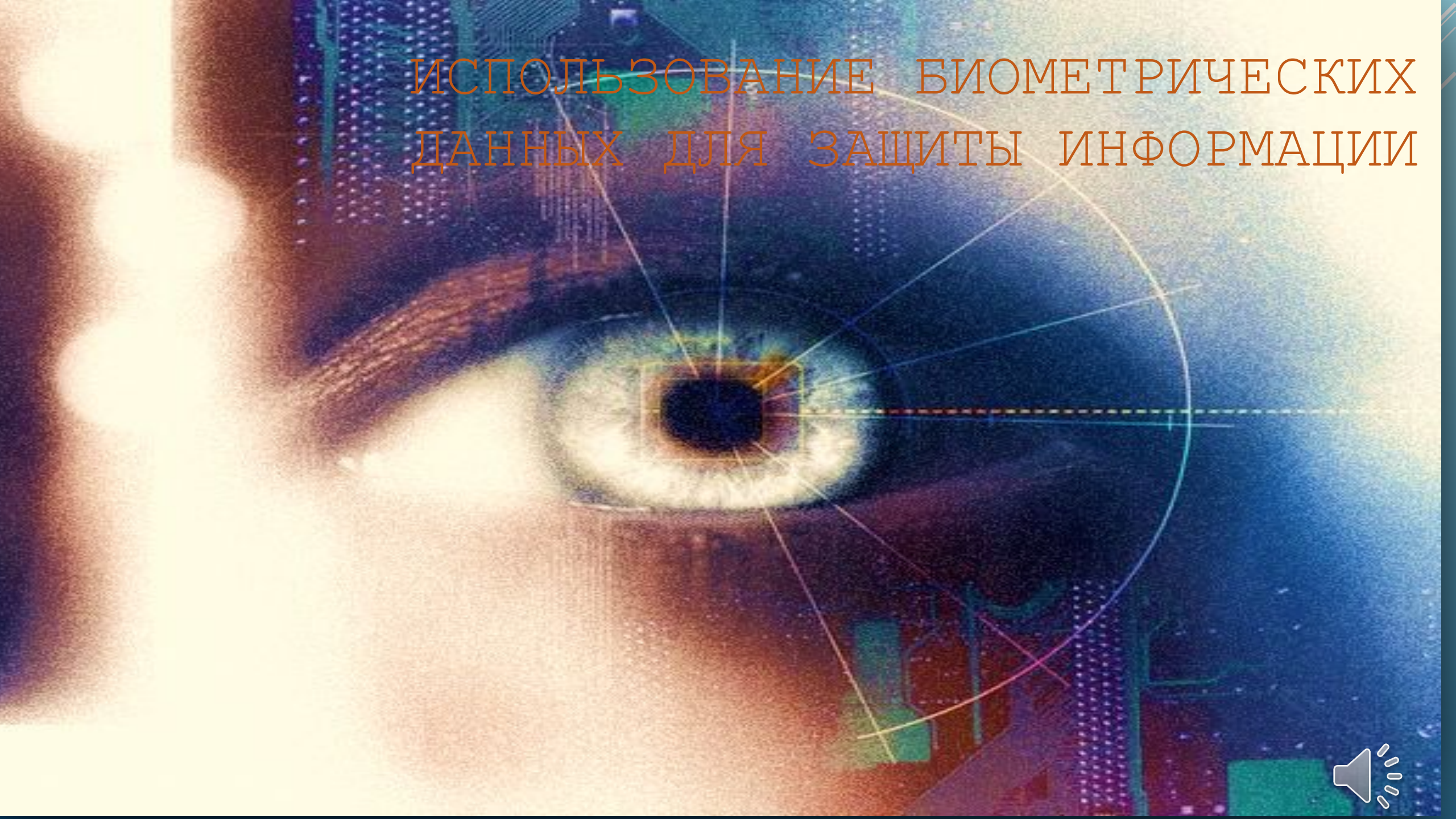


ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКИХ ДАННЫХ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Биометрические данные — это физиологические и биологические особенности человека, на основании которых можно установить его личность. Они применяются уже очень давно в различных сферах жизни, в том числе и в повседневности (мы узнаем знакомого человека по голосу, походке, лицу и пр.). С развитием информационных технологий биометрию стали внедрять и для идентификации пользователей в этой области.

ВСЕ СИСТЕМЫ ЗАЩИТЫ И КОНТРОЛИРУЕМОГО ДОСТУПА МОЖНО РАЗДЕЛИТЬ НА ТРИ ГРУППЫ:

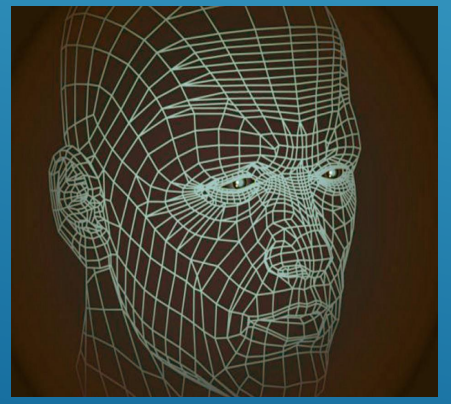
1. Парольная защита. В этом случае пользователь должен предъявить секретный PIN-код или пароль.
2. Ключи. Подразумевается физический носитель секретного ключа, который пользователь должен предъявить системе. Часто в этих целях используется пластиковая карта с магнитной полосой.
3. Биометрические данные. Чтобы получить доступ, пользователь должен предъявить параметр, который является частью его самого. При такой системе идентификации подвергается сама личность, а точнее, его индивидуальные характеристики. Например, радужная оболочка глаза, отпечатки пальцев, рисунок линий на ладони и т.д.

Статистические методы:

Аутентификация по отпечатку пальца

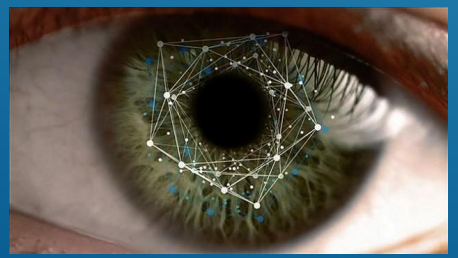
Аутентификация по геометрии руки

Аутентификация по геометрии лица



Аутентификация по радужной оболочке глаза

Аутентификация по сетчатке глаза



ДИНАМИЧЕСКИЕ МЕТОДЫ:

Аутентификация по голосу

Аутентификация по рукописному почерку

Аутентификация по походке

Рассмотрим круг задач, которые с успехом решаются с помощью новых технологий — биометрии:

- Вход в электронное рабочее место;
- Получение, передача конфиденциальной информации коммерческого характера;
- Ведение правительственных ресурсов;
- Осуществление банковских и финансовых операций;
- Торговля;
- Защита данных;
- Охрана правопорядка;
- Здравоохранение;
- Социальные услуги;
- Частная жизнь (умный дом, смартфоны).

Рассмотрим где и для чего используют биометрическую защиту:

- Контроль и учет рабочего времени;
- Охранные системы информационных ресурсов, доступа в образовательные и иные учреждения, дома, офисы,
- Криминалистика и спецслужбы;
- Банковская и финансовая сфера;
- Безопасность аэропортов;
- Метро;
- В промышленности предотвращение шпионажа, с целью завладения коммерческой тайны;
- Система голосования;
- Миграционные службы.

Если вы решили оборудовать свой офис, предприятие или дом этими самыми современными устройствами защиты, прислушайтесь к советам специалистов:

- Проведите анализ коммерческой необходимости этого, просчитайте экономическую целесообразность, рентабельность, предполагаемые преимущества внедрения оборудования.
- Не пренебрегайте мнением ваших сотрудников по вопросам нововведений, неприятие реформ может свести на нет ваши усилия и решения. Действуйте убеждением, а не авторитаризмом.
- Обратитесь к специалистам с хорошими рекомендациями, чтобы поручить им весь комплекс работ: проектирование, закупку оборудования и программных средств, монтаж, обучение персонала, обслуживание.
- Учитывайте, что рынок биометрических систем безопасности чрезвычайно быстро развивается, появляются новые, более дешевые и надежные образцы, а существующие устаревают морально раньше, чем изнашиваются.
- Решите вопрос, где будут храниться биометрические характеристики, так как при несанкционированном доступе к ним, краже или порче, новые данные для конкретного лица получить невозможно, они уникальны.
- Не следует применять только биометрическую защиту информации, задействуйте и более проверенные временем методы — пароли, карточки, жетоны, чипы и пр.

Биометрические системы будущего

В настоящее время разрабатывается целый ряд биометрических систем, которые на первый взгляд кажутся нереальными. Это использование запаха тела человека, отпечатка ноги человека (установлено, что голая ступня может идентифицировать человека в 99,6% случаев), скорость и ритм нажатия клавиш при наборе компьютерного пароля (это может повысить надежность авторизации), вен на руке, формы ушей и носа, контуров и зон опоры человеческой спины и многого другого. Пока остается непонятным, как такие характеристики могут обеспечивать точность в авторизации, но вполне вероятно, что придет время, и мы уже будем использовать их в повседневной жизни.


Спасибо за внимание