

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Прикладные информационные технологии» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОГО ЗАДАНИЯ №12**

**В РАМКАХ ДИСЦИПЛИНЫ «**[**БИОМЕТРИЧЕСКИЕ СИСТЕМЫ АУТЕНТИФИКАЦИИ**](https://online-edu.mirea.ru/course/view.php?id=5957)**»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Ответе на вопросы.  
**1. Основные методы биометрической идентификации**

Биометрическая идентификация использует уникальные физиологические или поведенческие характеристики человека. Основные методы:  
- Физиологические:  
 Отпечатки пальцев.  
 Радужная оболочка глаза.  
 Сетчатка глаза.  
 Геометрия лица (2D и 3D).  
 Геометрия кисти руки.  
- Поведенческие:  
 - Голос.  
 - Подпись.  
 -Клавиатурный почерк.

**2. Классификация биометрических средств защиты информации (ЗИ)**

Биометрические средства можно классифицировать:  
1. По типу идентифицируемых характеристик:  
 - Физиологические.  
 - Поведенческие.  
2. По степени точности:  
 - Высокоточные (радужная оболочка, отпечатки пальцев).  
 - Умеренно точные (лицо, голос).  
3. По способу применения:  
 - Однофакторные.  
 - Многофакторные (сочетание нескольких методов).

3. **Классификация биометрических методов информационной безопасности (ИБ)**

1. По используемым биометрическим признакам

Физиологические.

Поведенческие.

2. По способу взаимодействия

Контактные: требуют физического взаимодействия с устройством (например, сканер отпечатков пальцев).

Бесконтактные: используют дистанционные методы (например, сканирование лица или радужки глаза).

3. По типу обработки данных

Локальная обработка: данные обрабатываются и хранятся на устройстве пользователя.

Централизованная обработка: данные обрабатываются на удаленных серверах (например, в облаке).

4. По области применения

Государственная безопасность:

Системы идентификации и верификации граждан (например, Единая биометрическая система России).

Пограничный контроль.

Корпоративная безопасность:

Контроль доступа на предприятия.

Защита конфиденциальной информации.

Бытовые устройства:

Системы защиты смартфонов, планшетов, ноутбуков.

Умные дома.

5. По степени интеграции

Узкоспециализированные: системы, предназначенные для решения одной задачи (например, вход в здание).

Комплексные: многозадачные системы, интегрирующие несколько видов биометрии и другие методы ИБ.

6. По целям применения

Идентификация: определение личности из базы данных.

Аутентификация: подтверждение личности на основе сравнения с ранее зарегистрированным шаблоном.

**4. Системы по отпечаткам пальцев**

Физические характеристики пальца для составления биометрического шаблона:  
- Узоры на коже (дуги, петли, завитки).  
- Минуции (разветвления, окончания линий).  
- Поры и микродетали рисунка.

**5. Преимущества и недостатки метода отпечатков пальцев**

Преимущества:  
- Высокая точность.  
- Быстрая проверка.  
- Стабильность шаблона на протяжении жизни.  
Недостатки:  
- Чувствительность к повреждениям кожи.  
- Возможность подделки.  
- Ограничения при влажных или загрязненных пальцах.

**6. Системы по голосу**

Физические характеристики шаблона:  
- Частота и тембр голоса.  
- Особенности речевого аппарата.  
- Интонация.  
Преимущества:  
- Простота использования.  
- Не требуется физический контакт.  
Недостатки:  
- Чувствительность к шуму.  
- Изменения голоса при болезнях.  
- Более низкая точность по сравнению с физиологическими методами.

**7. Системы по радужной оболочке глаза**

Преимущества:  
- Исключительная уникальность рисунка.  
- Высокая устойчивость к подделкам.  
- Низкая вероятность ошибки.  
Недостатки:  
- Требуется специализированное оборудование.  
- Возможны ошибки при сильном освещении или движении глаз.

**8. Основные подсистемы системы идентификации по радужной оболочке глаза**

1. Сканирование радужной оболочки: Получение изображения.  
2. Обработка изображения: Выделение уникальных особенностей.  
3. Сравнение шаблонов: Сопоставление с базой данных.  
4. Принятие решения: Определение успешности идентификации.  
  
Статистические характеристики:  
- Низкий уровень ложного принятия (<0.0001%).  
- Высокая скорость обработки данных.

**9. Системы идентификации и аутентификации по изображению лица**

Классификация методов:  
1. Геометрические методы: используют расстояния между ключевыми точками (глаза, нос, рот).  
2. Методы текстурного анализа: исследуют особенности кожи.  
3. Методы глубокого обучения: выявляют сложные паттерны в изображении.

**10. Системы идентификации по 2D-изображению лица**

Преимущества:  
- Простота установки и использования.  
- Возможность работы на дистанции.  
Недостатки:  
- Зависимость от освещения и угла съемки.  
- Уязвимость к фотографиям и подделкам.

**11. Особенности систем по 3D-распознаванию лица**

Классификация систем:  
1. Активные: используют проекторы и датчики для создания модели лица.  
2. Пассивные: анализируют естественные 3D-структуры.  
Особенности:  
- Более высокая точность по сравнению с 2D-методами.  
- Устойчивость к изменениям освещения.  
- Сложность и высокая стоимость оборудования.