

**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 №6**

**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.

**1 Перечислите основные нормативные и справочные документы, регламентирующие работу с биометрическими системами идентификации/аутентификации.**

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»
2. Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
3. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
4. Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
5. Постановление Правительства Российской Федерации от 13.02.2019 № 146 «Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных»
6. Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»

**2 Рассмотрите и представьте в отчете критерии биометрической идентификации.**

1. Всеобщность: каждый человек имеет биометрические характеристики;
2. Уникальность: для биометрии нет двух людей, обладающих одинаковыми биометрическими характеристиками;
3. Постоянство: биометрические характеристики должны быть стабильны во времени;
4. Изменяемость: биометрические характеристики должны быть измеряемы каким-либо физическим считывающим устройством
5. Приемлемость: совокупность пользователей и общество в целом не должны возражать против измерения/сбора биометрических параметров

**3 Приведите примеры (не менее 3) использования биометрической идентификации в различных устройствах (как указано в таблице)**

|  |  |  |  |
| --- | --- | --- | --- |
| Название системы | Suprema BioLite N2 | Diebold Nixdorf Iris Scanner ATM | Hikvision DeepinMind NVR |
| Биометрический параметр | Отпечаток пальца | Радужная оболочка глаза | Лицо |
| Вид системы | Контроль доступа (папиллярные узоры) | Банковские терминалы | Система видеонаблюдения |
| Разработчик | Suprema Inc. | Diebold Nixdorf | Hikvision |
| Название устройства | BioLite N2 | Diebold Nixdorf Scanner | DeepinMind MVR |
| Принцип действия | Сканирование папиллярных узоров | Сканирование радужной оболочки глаза | Распознавание лиц на основе машинного обучения |
| Стоимость | От 500 $ | От 1000 $ | От 1200 $ |
| Сайт производителя | [supremainc.com](https://vk.com/away.php?to=https%3A%2F%2Fsupremainc.com&utf=1) | [dieboldnixdorf.com](https://vk.com/away.php?to=https%3A%2F%2Fdieboldnixdorf.com&utf=1) | [hikvision.com](https://vk.com/away.php?to=https%3A%2F%2Fhikvision.com&utf=1) |

**4 Сформулируйте и представьте в отчете угрозы взлома биометрических систем. Приведите примеры**

Подделка биометрических данных (спуфинг)

Биометрические системы уязвимы к атаке, в которой злоумышленники используют поддельные биометрические данные для получения несанкционированного доступа.  
  
Пример: Подделка отпечатков пальцев с использованием высококачественных снимков пальцев может обойти сканеры, если система не оснащена механизмами обнаружения живости, как это было продемонстрировано на различных моделях устройств.

Атаки с использованием фотографий или 3D-моделей (Replay-атаки)

Фотографии, видео или модели, воспроизводящие лица или другие биометрические данные, могут использоваться для обмана системы распознавания.  
  
Пример: Устройства распознавания лица могут обманываться 3D-масками или даже фотографиями высокого разрешения. Например, исследователи обнаружили, что некоторые модели смартфонов уязвимы к распознаванию лица через фотографии владельцев.

Атаки на каналы связи и базы данных

Поскольку биометрические данные передаются между различными устройствами и хранятся в базах данных, они могут быть уязвимы к перехвату и модификации.  
  
Пример: Если канал связи не зашифрован должным образом, то перехваченные биометрические данные могут быть использованы для воспроизведения атаки. В прошлом атаки на банковские терминалы уже включали перехват биометрических данных, что позволяло злоумышленникам копировать и повторно использовать данные для создания поддельных шаблонов.

Атаки на программное обеспечение и аппаратные уязвимости

Системы биометрии зависят от сложных алгоритмов и датчиков, которые могут быть подвержены ошибкам или уязвимостям, позволяя злоумышленникам манипулировать данными.  
  
Пример: Атаки на нейросетевые алгоритмы, такие как атака с изменением изображения (adversarial attacks), могут сбивать системы распознавания лиц, заставляя их воспринимать людей как других.

Кража биометрических данных

В случае взлома хранилищ с биометрическими данными утечка этих данных является невосстанавливаемой угрозой, так как биометрические признаки не могут быть изменены, как, например, пароли.  
  
Пример: Кража данных отпечатков пальцев или снимков радужной оболочки может позволить злоумышленникам создавать поддельные биометрические идентификаторы.