ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»

Дисциплина:

«Теория информационной безопасности и методология защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

Разграничение доступа. Идентификация и аунтификация

Выполнили:

Соловьев Артемий Александрович

Гр. P32151

Проверил:

Аспирант ФБИТ

Кондратенко Станислав Сергеевич

Санкт-Петербург

2023г.

Цель:

Разработка подсистемы идентификации и аунтификации субъектов.

Задачи:

1. составить алгоритм для реализации выбранной подсистемы.
2. Составить полную схему компьютерной системы со встроенной в нее подсистемой идентификации и аунтификации.

Ход работы:

- Конспект (Биометрическая идентификация и аунтификация)

Биометрическая идентификация и аутентификация — это процессы использования уникальных физиологических или поведенческих характеристик человека для определения его личности.

В качестве биометрических характеристик, которые могут быть использованы при аутентификации субъекта доступа, достаточно часто применяют следующие:

1. отпечатки пальцев;
2. геометрическая форма рук;
3. форма и размеры лица;
4. особенности голоса;
5. биомеханические характеристики почерка;
6. биомеханические характеристики «клавиатурного почерка».

Плюсы подсистемы:

1. **Надежность**: Биометрические характеристики уникальны для каждого человека, что делает идентификацию и аутентификацию более надежными по сравнению с традиционными методами, такими как пароли или пин-коды.
2. **Удобство использования**: Биометрические системы удобны в использовании, поскольку они основаны на физиологических или поведенческих характеристиках, которые всегда с человеком.
3. **Быстрота и эффективность**: Процесс идентификации и аутентификации с использованием биометрических данных может быть выполнен очень быстро, практически в реальном времени.
4. **Устойчивость к подделке**: Биометрические характеристики сложно подделать, особенно если используются новейшие алгоритмы распознавания.

Минусы подсистемы:

1. **Проблемы конфиденциальности и защиты данных:** Существует риск хищения или несанкционированного использования этих данных, поэтому необходимы строгие меры безопасности для их защиты.
2. **Возможность ошибок при распознавании:** несмотря на высокую точность биометрических систем, существует возможность ложного срабатывания (false positives) или неверного распознавания (false negatives).
3. **Влияние внешних факторов:** старение, изменения веса или травмы, могут повлиять на точность биометрической идентификации и аутентификации.
4. **Зависимость от технического оборудования:** Внедрение биометрических систем требует наличия специального технического оборудования, такого как сканеры отпечатков пальцев, камеры для распознавания лица или сканеры сетчатки глаза.

Биометрические системы практически никогда не хранят непосредственные биометрические образы пользователей (например, отпечатки пальцев) и не выполняют сравнение с ними биометрических образов, предъявляемых на этапе аутентификации. Предъявляемый пользователем биометрический образ, как правило, преобразуется модулем регистрации в вектор биометрических признаков, который и обрабатывается в дальнейшем

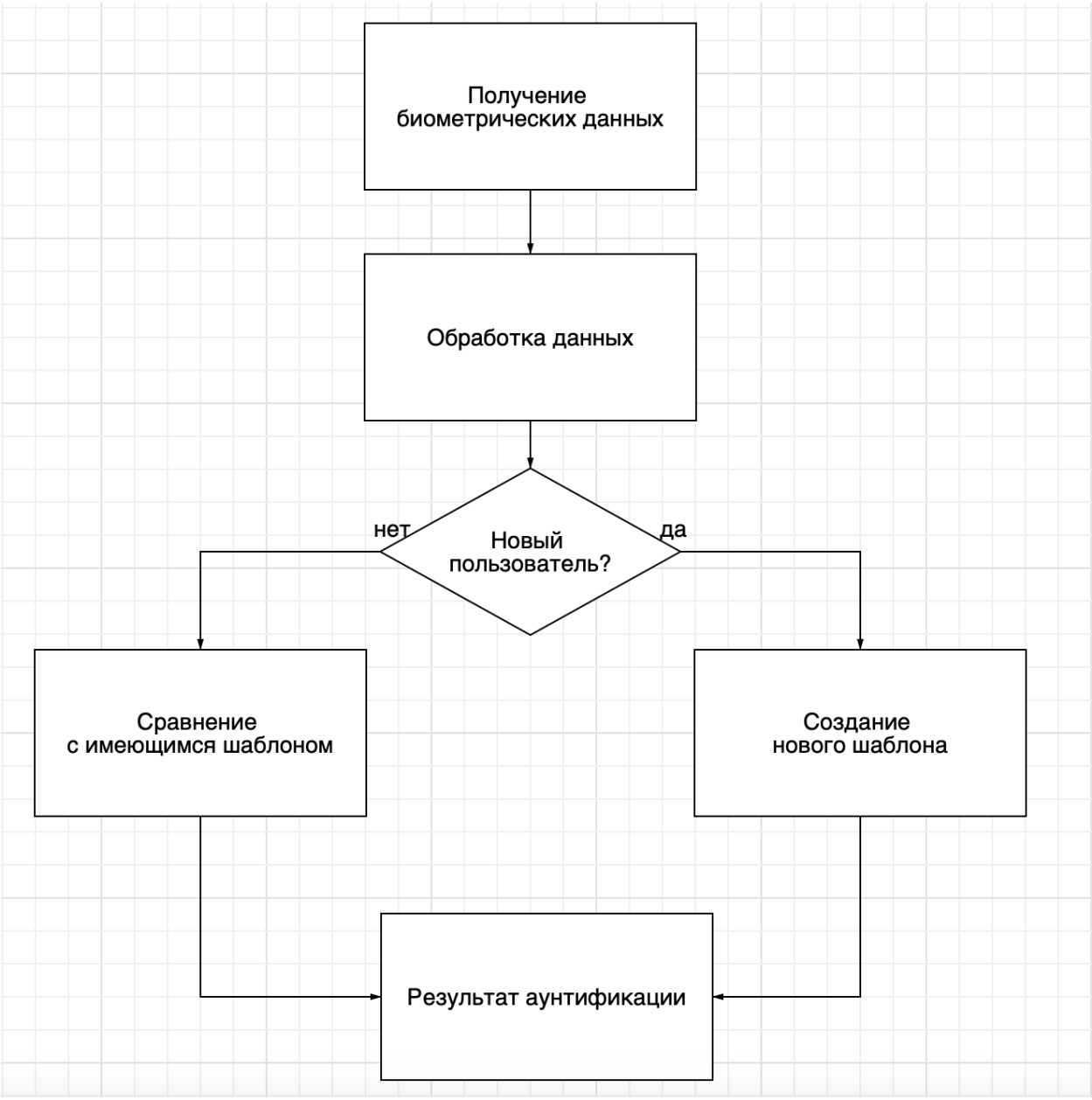

Рисунок 1.Алгоритм работы подсистемы

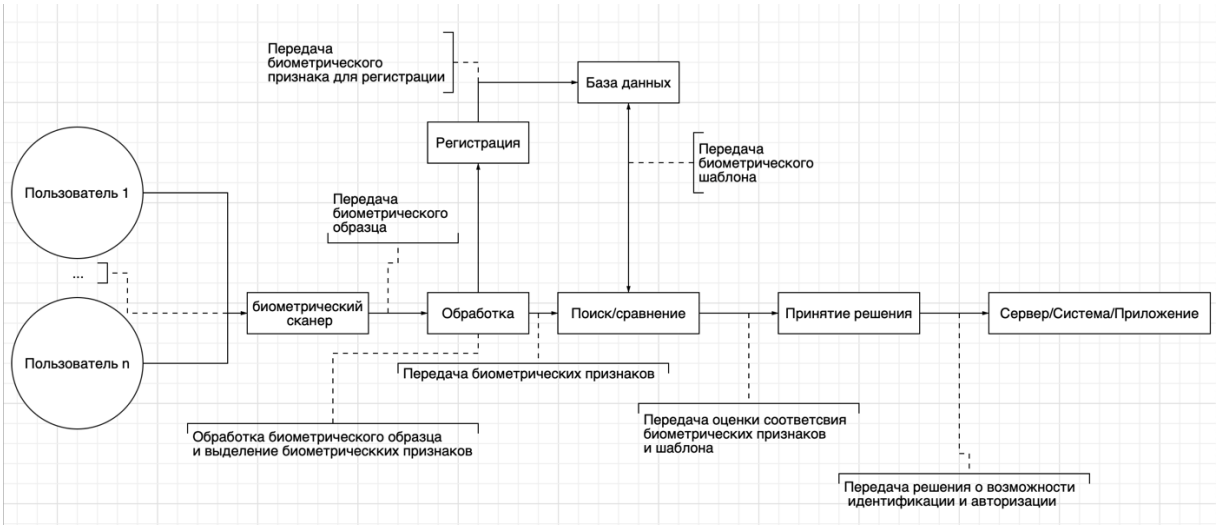

Рисунок 2.Схема компьютерной системы

Вывод:

В целом модель безопасности с биометрической подсистемой аунтификации и идентификации имеет высокий уровень безопасности, но требует затрат на техническое оборудование и необходимость постоянного обновления систем безопасности во избежание утечек биометрических данных пользователей.