|  |  |
| --- | --- |
| Gerb-BMSTU_01 | **Министерство науки и высшего образования Российской Федерации**  **Федеральное государственное бюджетное образовательное учреждение**  **высшего образования**  **«Московский государственный технический университет**  **имени Н.Э. Баумана**  **(национальный исследовательский университет)»**  **(МГТУ им. Н.Э. Баумана)** |

ФАКУЛЬТЕТ **Информатика и системы управления**

КАФЕДРА **Компьютерные системы и сети (ИУ6)**

НАПРАВЛЕНИЕ ПОДГОТОВКИ 09.03.03 **Прикладная информатика**

**Отчет**

**по домашней работе**

**Дисциплина:** защита информации

Преподаватель  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** Д.А. Миков

(Подпись, дата) (И.О. Фамилия)

Студент гр. ИУ6-84Б **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** С.П. Пантелеев

(Подпись, дата) (И.О. Фамилия)

Москва, 2022

**Цель:** выявить риски нарушения целостности, доступности и/или конфиденциальности в заданной автоматизированной системе и разработать для нее политику безопасности.

Исследовать информационные процессы в заданной автоматизированной системе и предложить средства и методы для их защиты.

**Описание объекта защиты:** мобильное приложение для подбора одежды в соответствии с погодными условиями.

**Информация, задаваемая пользователем:**

* выбор шаблонной одежды;
* добавление собственной одежды;
* разрешение отслеживания геолокации;
* выбор настроек (шкала температуры, гендер и теплоощещение).

**Информация, выдаваемая пользователю:**

* температура (обычная, как ощущается, максимальная и минимальная);
* геолокация;
* одежда (картинка и подпись), которую можно одеть в соответствии с погодой;
* в гардеробе одежда отображается в соответствии с выбранным полом.

Можно выявить следующие информационные процессы в заданной программной системе:

1. Приложение получает информацию о погоде с open-source сайта openweather.
2. Пользователь получает подобранную одежду.
3. Добавление в базу данных новой и имеющейся одежды.
4. Сохранение настроек на устройстве пользователя.

Концептуальная модель безопасности представлена на рисунке 1.

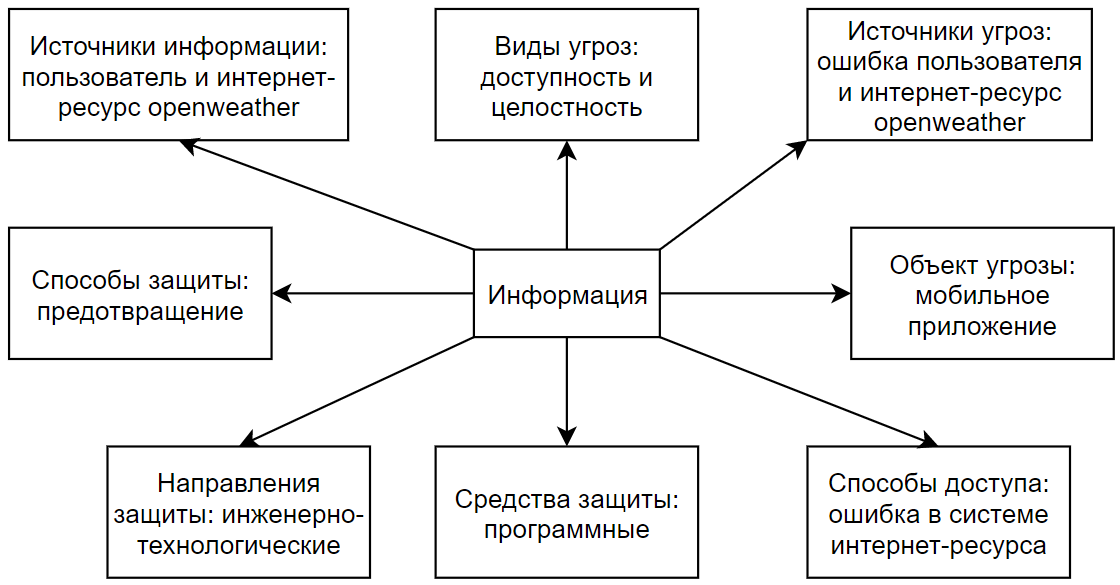


Рисунок 1 – концептуальная модель безопасности

Построенная модель позволяет выявить ряд проблем:

1. Проблема защиты пользователя от самого себя. Для этого нужен контроль за корректностью вводимой информации.
2. При добавлении новой одежды происходит добавление новых данных в БД, при отметке имеющейся одежды, происходит обновление уже имеющихся данных в БД. Для большей надежности можно базу данных перенести на сервер. А также можно делать резервные копии, чтобы была возможность откатиться к рабочей версии БД, в случае сбоя работы\целостности.
3. Данные, которые пользователь сохраняет в настройках, сохраняются один файлом на телефон. Для надежности, их хранения можно перенести на сервер.
4. Для предотвращения возможности перехвата данных, передаваемых от интернет-ресурса к приложению, следует использовать зашифрованный трафик. Например, можно использовать протокол HTTPS для обмена данными.

Подведенные итоги приведены в таблице 1.

Таблица 1 – Итоговые меры защиты

|  |  |  |
| --- | --- | --- |
| № | Проблема | Решение |
| 1 | Защита от пользователя | Проверка на корректность вводимой информации |
| 2 | Целостность БД | Перенос БД на сервер и создание резервных копий |
| 3 | Потеря настроек пользователя | Перенос данных на сервер |
| 4 | Несанкционированный доступ к данным | Использовать только шифрованный трафик |

**Вывод:** были выявлены риски нарушения целостности и доступности в заданной автоматизированной системе и разработана для нее политика безопасности.