**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Обеспечение информационной безопасности мобильных устройств»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

«Безопасность смартфонов Android, IOS и резервное копирование»

**Выполнили:**

Ахраров Али, студент группы N3350

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Федоров Иван Романович

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Содержание

[1. ВВЕДЕНИЕ 3](#_Toc191170022)

[2 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ МОБИЛЬНОГО УСТРОЙСТВА 4](#_Toc191170023)

[3 ЗАКЛЮЧЕНИЕ 7](#_Toc191170024)

[5. ПРИЛОЖЕНИЕ 8](#_Toc191170025)

1. ВВЕДЕНИЕ  
   Цель работы – обеспечить безопасность мобильного устройства на примере смартфона Xiaomi Redmi Note 9.  
   Для достижения цели необходимо решить следующие задачи:  
   − настроить автоматическую блокировку экрана;  
   − установить PIN-код SIM-карты;  
   − настроить шифрование данных;  
   − защитить приложение «Just» паролем с отключением уведомлений;  
   − создать резервную копию данных (облачное и локальное хранение);  
   − активировать функцию «Найти устройство»;  
   − проверить APK-приложение через сервис VirusTotal;  
   − провести проверку malware (на примере приложения «Just»), так как тестовый malware установить не удалось.

# 2 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ МОБИЛЬНОГО УСТРОЙСТВА

**1 Задание**   
Необходимо реализовать комплекс мер по защите мобильного устройства, включающий:  
− автоматическую блокировку экрана;  
− установку PIN-кода SIM-карты;  
− шифрование данных устройства;  
− защиту приложения «Just» паролем с отключением уведомлений;  
− резервное копирование данных (облачное и локальное);  
− активацию функции «Найти устройство»;  
− проверку APK-файлов и malware через сервис VirusTotal.

**1.2 Ход работы**

**1.2.1 Автоматическая блокировка экрана**  
В разделе «Настройки» → «Экран» установлено время бездействия 30 секунд, после которого экран автоматически блокируется. Это позволяет **оперативно защищать** данные при отсутствии активности.

**1.2.2 Разблокировка по лицу**  
Попытка настройки функции разблокировки по лицу выявила, что данная возможность отсутствует на Xiaomi Redmi Note 9.  
**Биометрическая разблокировка** – метод аутентификации с использованием физиологических характеристик, таких как лицо или отпечаток пальца.

**1.2.3 Установка PIN-кода SIM-карты**  
В разделе «SIM-карты и мобильные сети» активирована опция блокировки SIM-карты. После установки PIN-кода при каждом перезагружении устройства требуется ввод кода, что предотвращает несанкционированный доступ к мобильной связи.

**1.2.4 Шифрование данных**  
В настройках «Пароли и безопасность» подтверждено, что данные устройства зашифрованы по умолчанию. При необходимости возможна активация дополнительных параметров шифрования для защиты конфиденциальной информации.

**1.2.5 Защита приложения «Just»**  
Для защиты приложения «Just» использована встроенная функция **App Lock**.  
**1.2.5.1 Использование App Lock**  
Приложение «Just» было защищено паролем, что ограничивает несанкционированный доступ.  
**1.2.5.2 Отключение уведомлений**  
В настройках уведомлений для данного приложения отключён вывод информации на экран, что минимизирует риск утечки данных.

**1.2.6 Резервное копирование данных**  
Резервное копирование выполнено двумя способами:  
− **Облачное резервное копирование:** через Mi-аккаунт, при котором сохраняются контакты, настройки и медиафайлы;  
− **Локальное резервное копирование:** посредством подключения устройства к компьютеру с последующим копированием важных файлов.

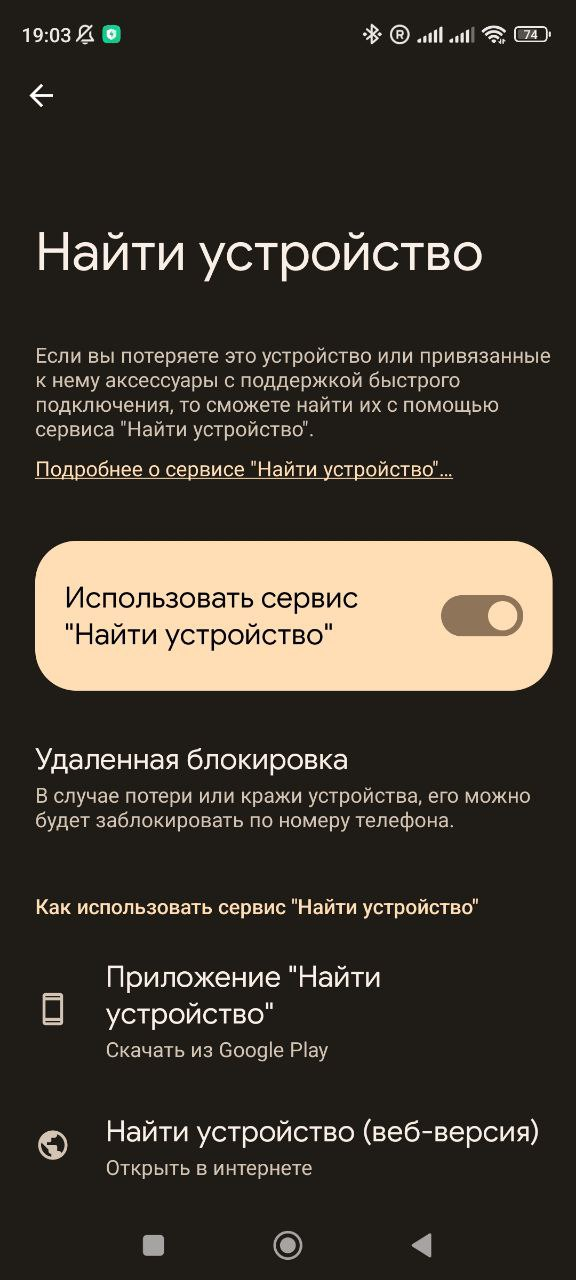
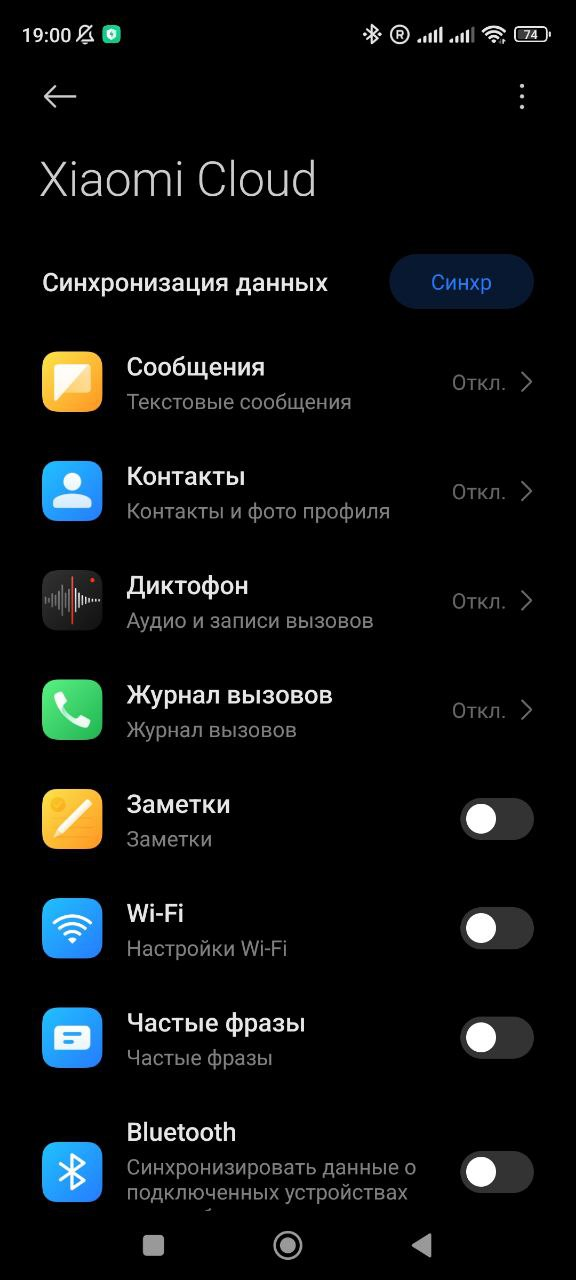
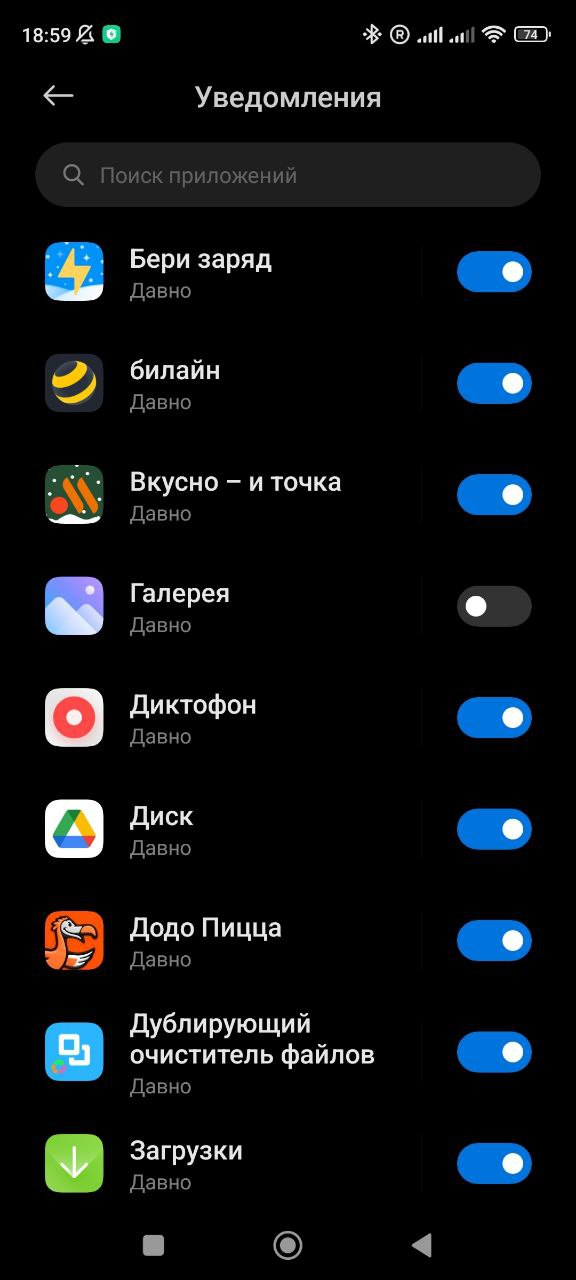
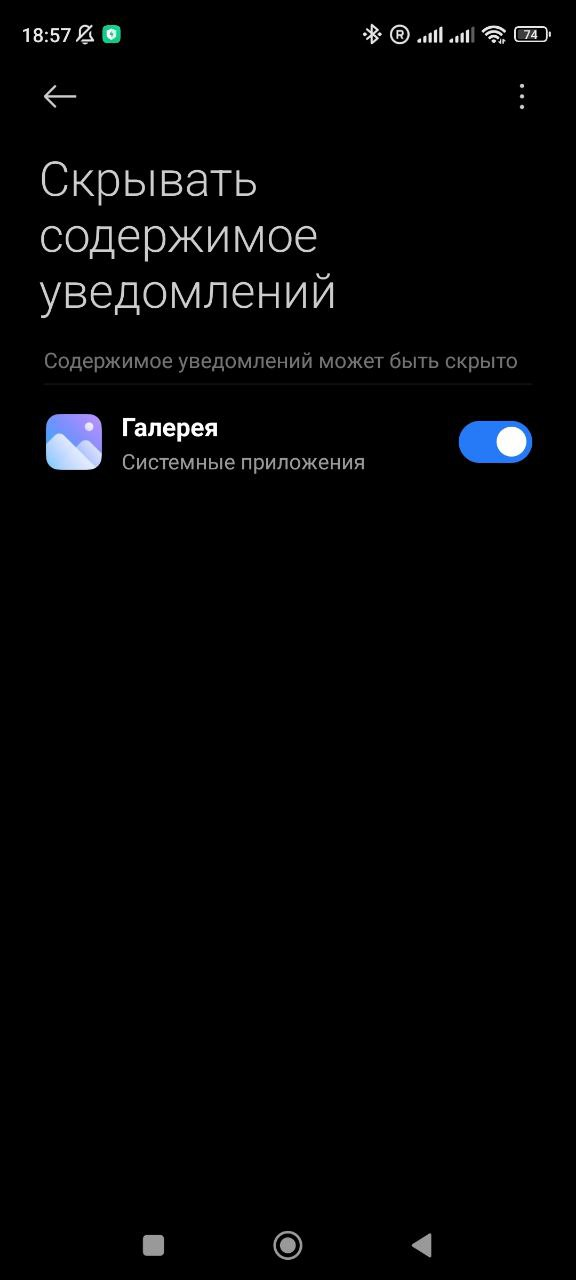
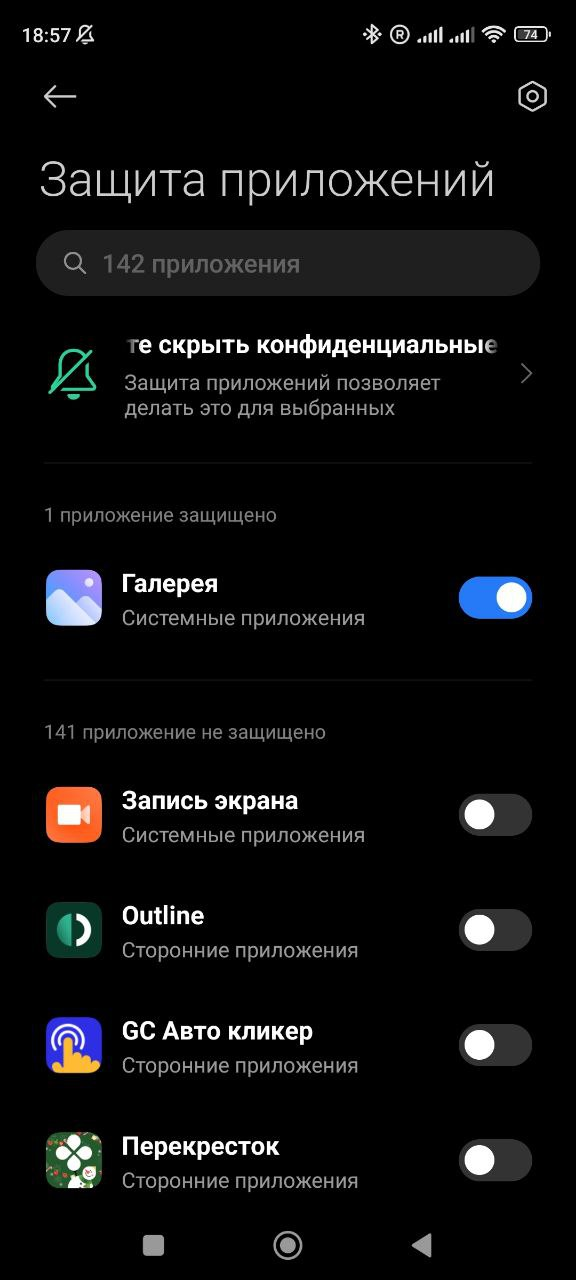
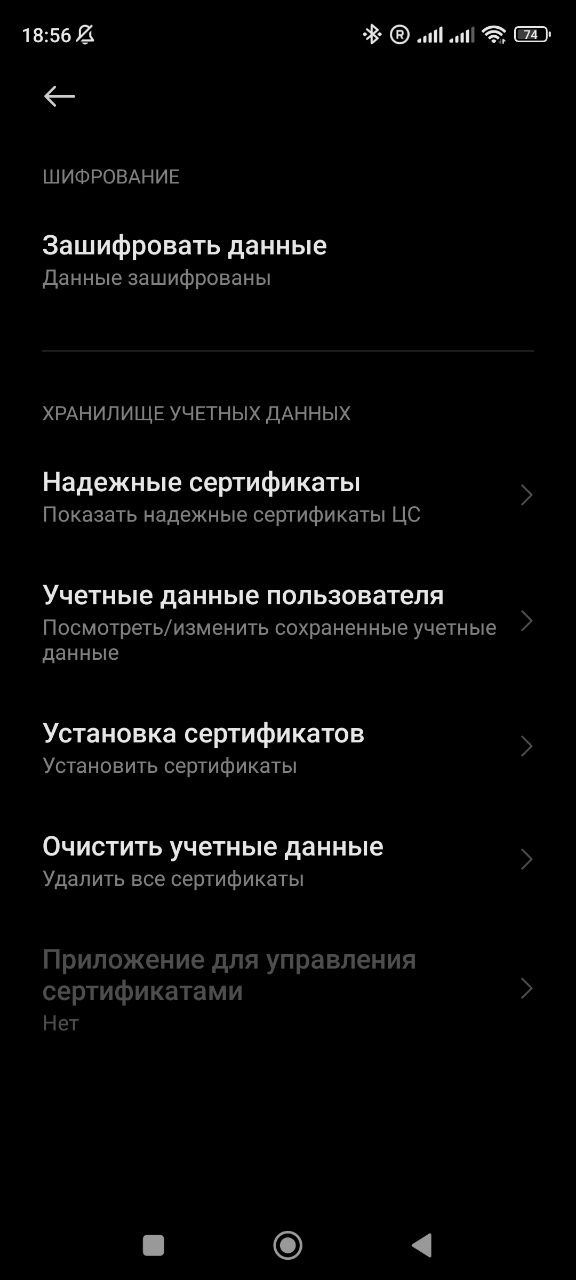
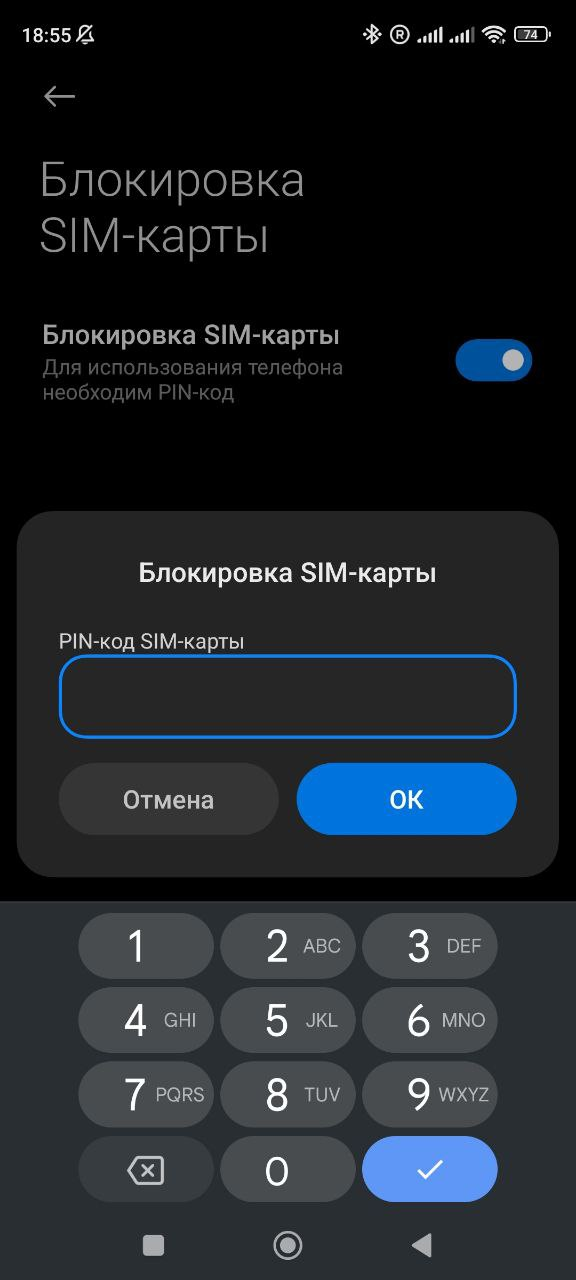
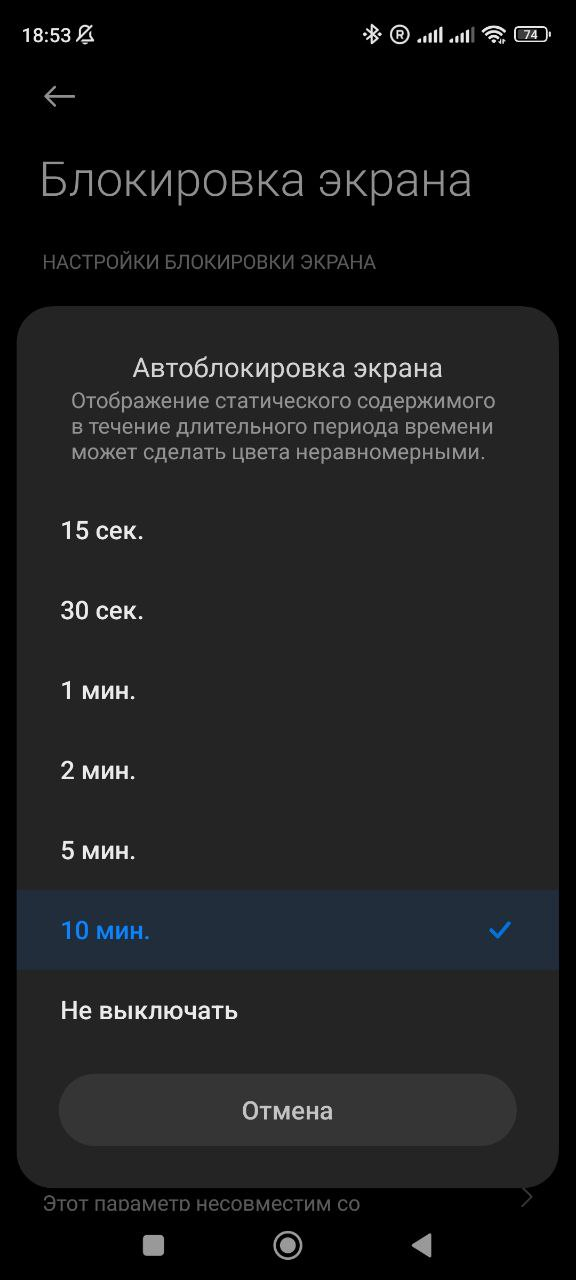
**1.2.7 Активация функции «Найти устройство»**  
Функция «Найти устройство» активирована через Mi-аккаунт. Это позволяет в случае утраты смартфона отследить его местоположение, а также дистанционно заблокировать или удалить данные.

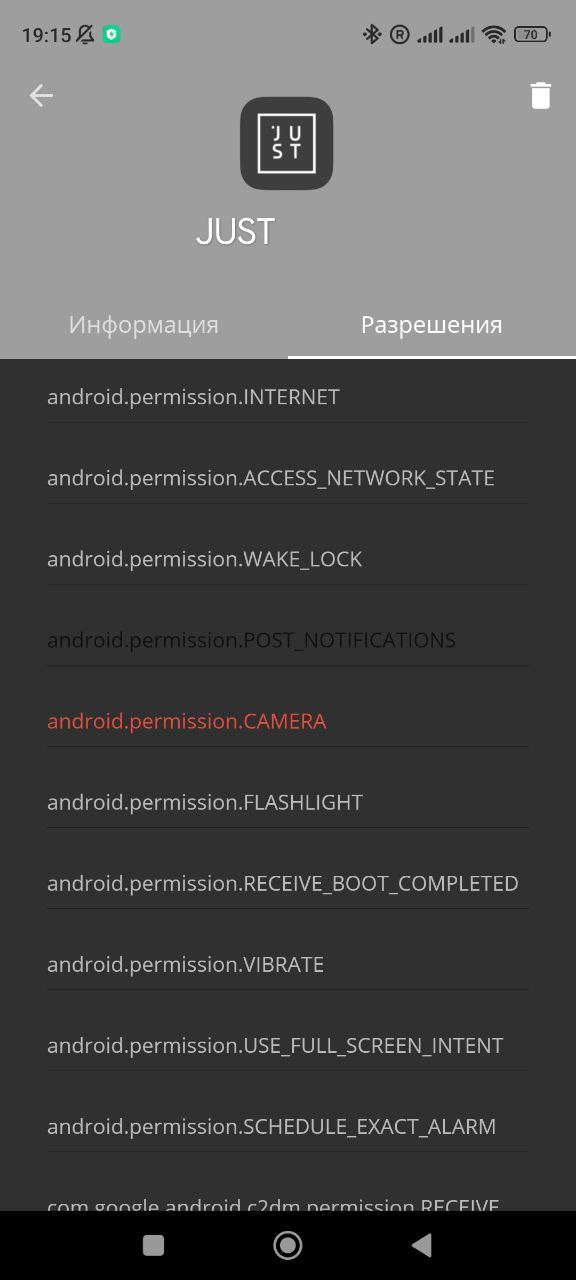
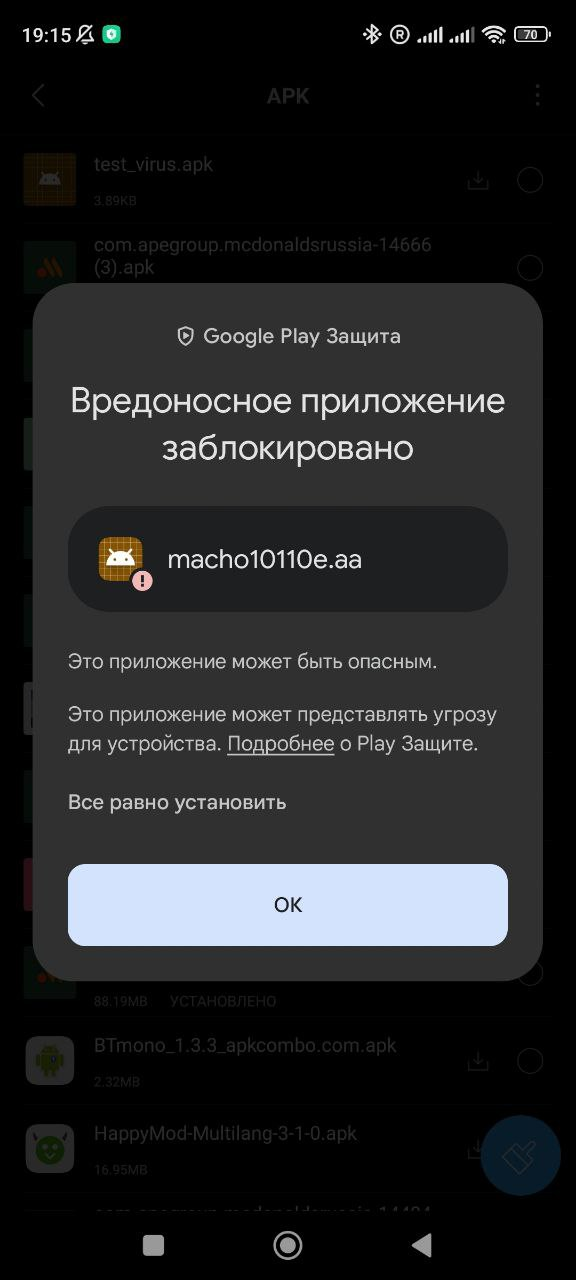
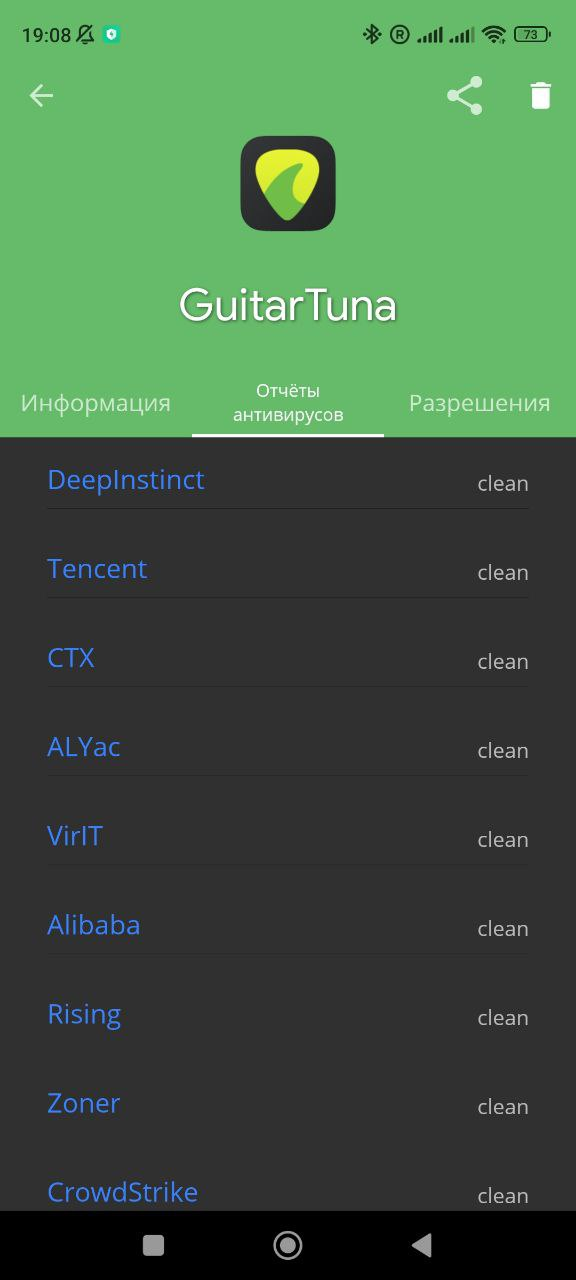
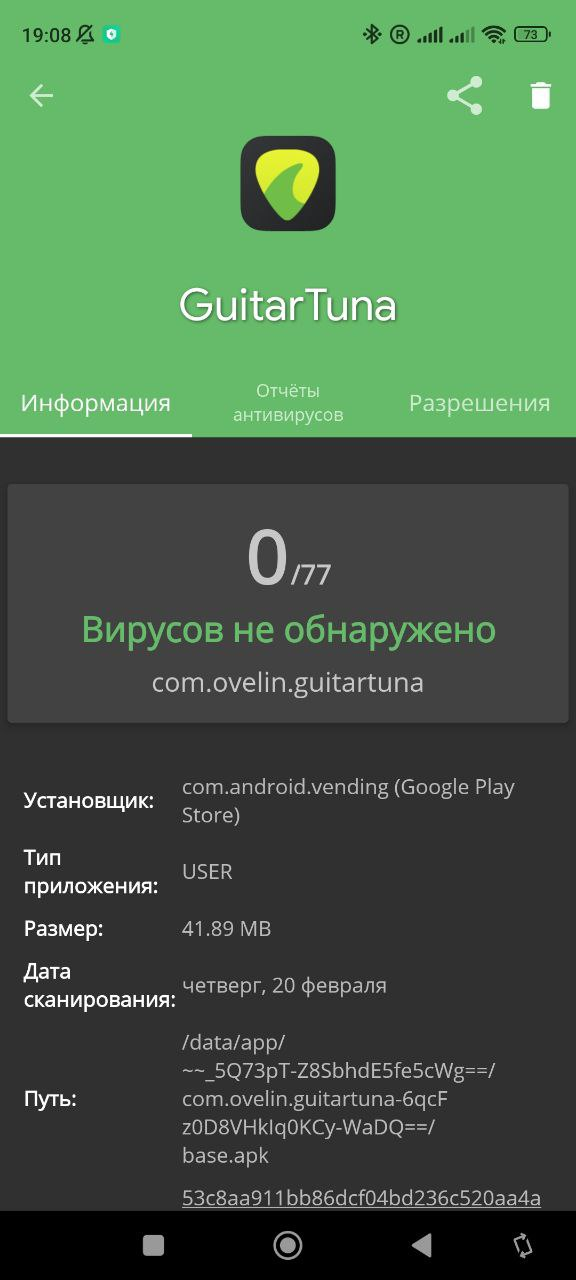
**1.2.8 Проверка APK-приложения через VirusTotal**  
Выбран APK-файл (не относящийся к malware) был загружен на сервис VirusTotal. Результаты анализа показали, что антивирусные движки не выявили угроз, что свидетельствует о корректности файла.

**1.2.9 Проверка malware (на примере приложения «Just»)**  
При попытке установки тестового malware система заблокировала его установку. В качестве примера для анализа было использовано приложение «Just».  
1.2.9.1 Анализ через VirusTotal  
При загрузке файла приложения «Just» на VirusTotal зафиксировано срабатывание нескольких антивирусных систем, что указывает на наличие подозрительных элементов.  
Пример ссылки на таблицу (таблица А.1).

**1.2.10 Сравнение результатов проверки**  
Сравнение показало, что:  
− обычные APK-приложения проходят проверку без срабатываний антивирусных систем;  
− приложение «Just» вызывает предупреждения, что подтверждает эффективность реализованных мер безопасности.

1. ЗАКЛЮЧЕНИЕ  
   Было выполнено: настройка автоматической блокировки экрана, установка PIN-кода SIM-карты, шифрование данных, защита приложения «Just» паролем с отключением уведомлений, создание резервных копий данных и активация функции «Найти устройство».  
   Эти мероприятия позволили получить навыки комплексного обеспечения безопасности мобильных устройств. Проверка через VirusTotal выявила отсутствие угроз у стандартных APK-файлов и обнаружение подозрительных элементов в приложении «Just», что свидетельствует о работоспособности применённых мер.

5. ПРИЛОЖЕНИЕ  




Скриншоты:

1. Параметры автоматической блокировки экрана (установка времени ожидания);
2. Включение блокировки SIM-карты и ввод PIN-кода;
3. Раздел «Безопасность» с опцией шифрования данных.
4. Встроенная функция «Защита приложений» (App Lock) для установки пароля;
5. Опция «Скрывать содержимое уведомлений» для защищаемых приложений;
6. Общий список приложений с возможностью управления уведомлениями.
7. Раздел «Xiaomi Cloud» с настройками синхронизации и резервного копирования данных;
8. Активация сервиса «Найти устройство», позволяющего при потере телефона отследить его местоположение и выполнить дистанционную блокировку или очистку.
9. Проверка приложения «GuitarTuna» в сервисе VirusTotal (0/77 — вирусов не обнаружено);
10. Предупреждение системы о блокировке вредоносного приложения (macho10100.apk);
11. Анализ приложения «Just» в VirusTotal, при котором обнаружены потенциально опасные разрешения или компоненты.