РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ

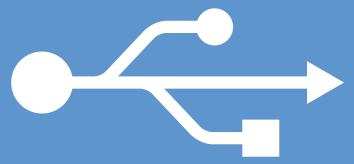
КАФЕДРА КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

выпускная квалификационная работа

РАЗРАБОТКА СПОСОБА ПРОТИВОДЕЙСТВИЯ АТАКАМ, ОСУЩЕСТВЛЯЕМЫМ С ПОМОЩЬЮ УСТРОЙСТВ, ПОДКЛЮЧАЕМЫХ ЧЕРЕЗ ИНТЕРФЕЙС USB

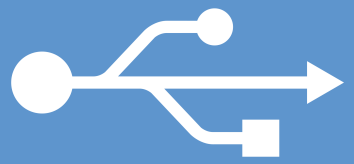
ВЫПОЛНИЛ: Ю.Р. Мамедов, ФИСБ4-КЗОИ

НАУЧНЫЙ РУКОВОДИТЕЛЬ: А.С. Забабурин



Целью данной работы является разработка эффективного способа противодействия атакам осуществляемым через интерфейс USB.

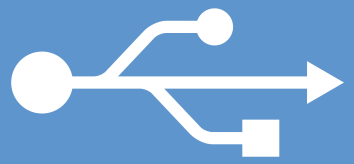
АКТУАЛЬНОСТЬ



Интерфейс USB (универсальная последовательная шина) широко распространен во всех областях в которых используется компьютерная техника.

Каждое современное компьютерное устройство поддерживает данный интерфейс, следовательно атакам реализуемым с его использованием подвержено почти каждое устройство.

РЕШАЕМЫЕ ЗАДАЧИ



1. Провести анализ интерфейса USB и HID-устройств.
2. Изучить и воспроизвести атаку типа BadUSB.
3. Рассмотреть способы противодействия атакам типа BadUSB.
4. Разработать утилиту, реализующую идентифицированные подходы к контролю доступа к портам;
5. Предложить подход к созданию программно-аппаратного комплекса контроля доступа к USB-портам.

USB ИНТЕРФЕЙС

USB – это промышленный стандарт, разработанный в середине 1990-х годов, который определяет кабели, разъемы и коммуникационные протоколы, используемые для подключения и электропитания между компьютерами и электронными устройствами.

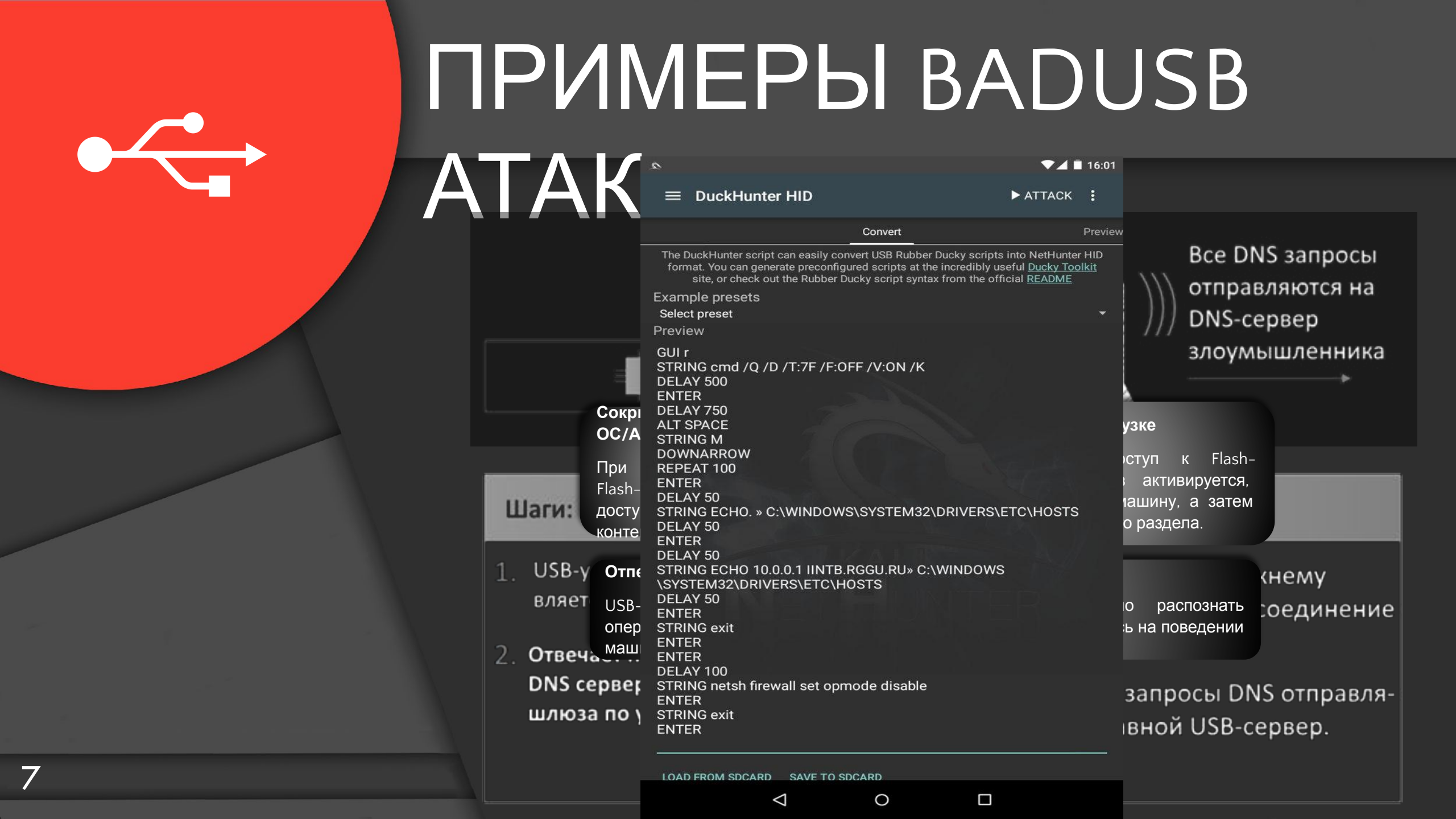
Работой устройства управляет записанная в микроконтроллер производителем микропрограмма – она определяет такие данные как:

- Тип устройства
- Необходимый драйвер
- Наименование производителя
- И т.д.

АТАК УЯЗВИМОСТЬ BADUSB

BadUSB пользуется тем фактом, что производители не защищают свои устройства от перезаписи или обновления микропрограммы, а хосты не проверяют USB устройства на подлинность. Благодаря этому злоумышленник может перепрограммировать микроконтроллер и выдать одно устройство за другое.

ПРИМЕРЫ BADUSB АТАК



СРЕДСТВА ЗАЩИТЫ

Несмотря на высокую сложность обнаружения вредоносного USB-устройства существуют некоторые предупреждающие методы защиты. Они не могут гарантировать полную защиту от данной уязвимости, однако с их помощью можно предотвратить атаки, направленные непосредственно на загруженную и работающую ОС.

Среди методов контроля реализуемых средствами ОС, можно перечислить следующие:

- Разграничение доступа к системному реестру
- Контроль INF файлов хранящих информацию необходимую для установки устройств.
- Защита средствами групповых политик Windows.

«USB GUARD»

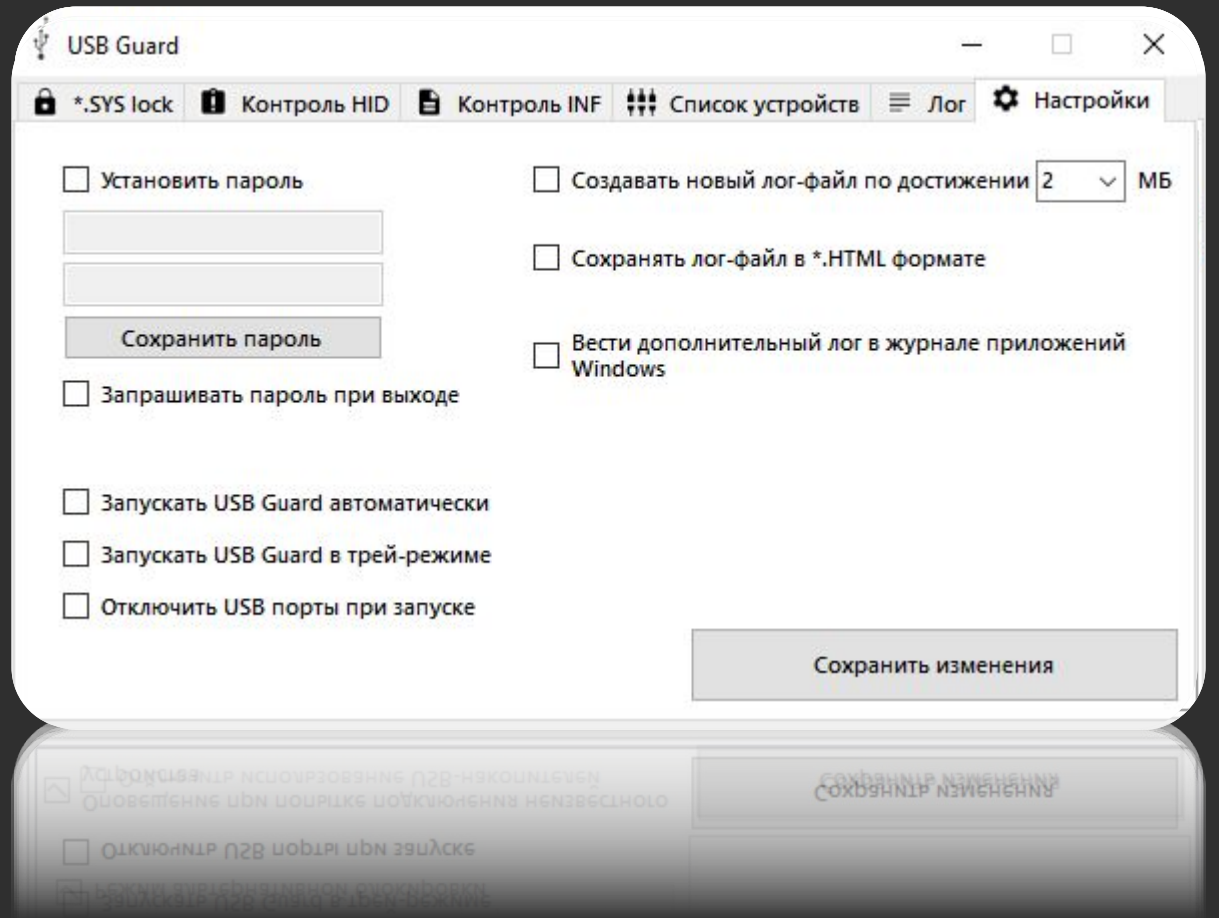
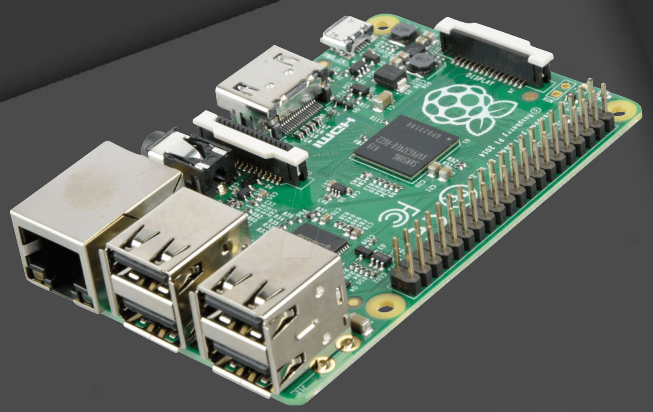
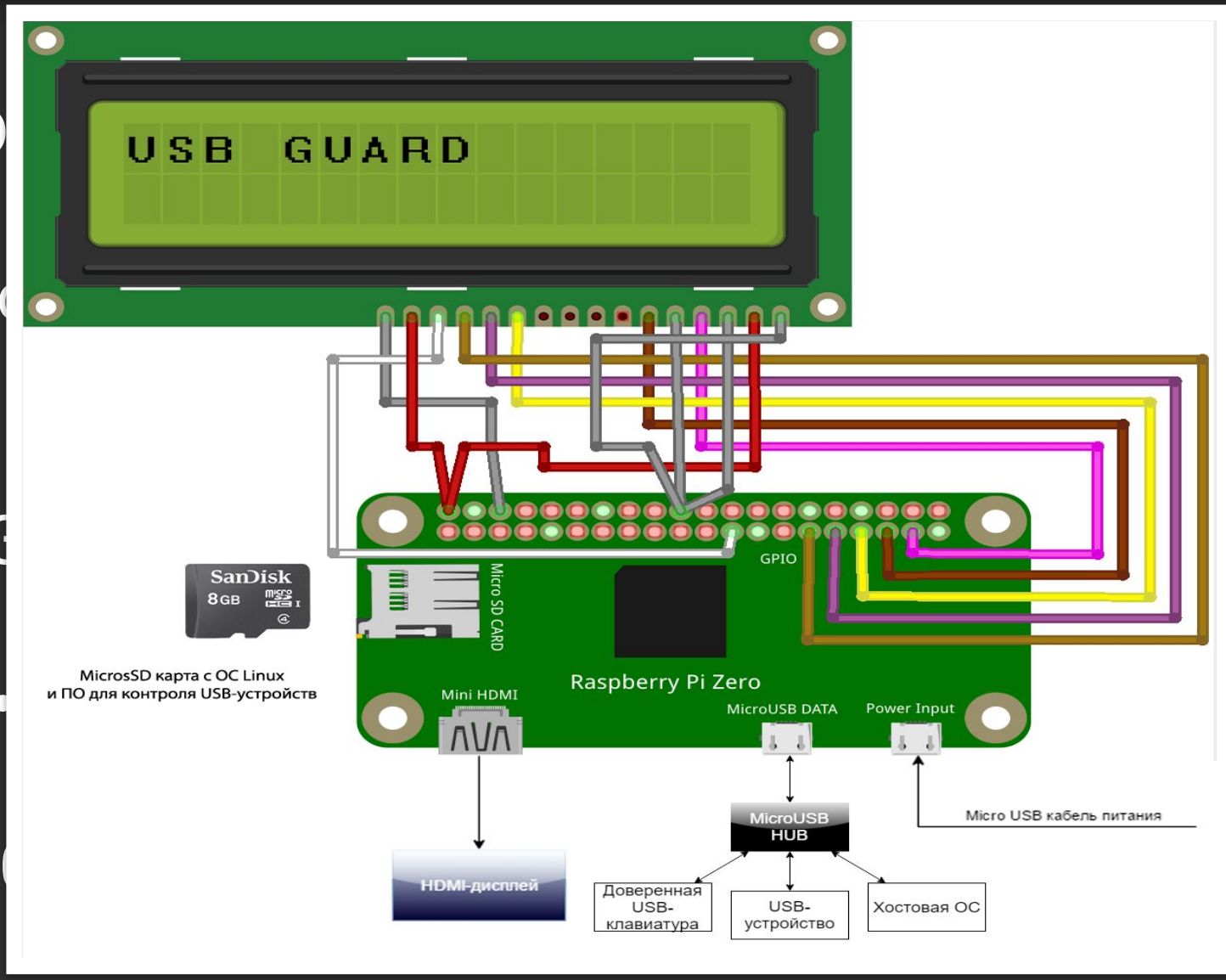

USB Guard
*.SYS lock
Контроль HID
Контроль INF
Список устройств
Лог
Настройки
Установить пароль
Сохранить пароль
Запрашивать пароль при выходе
Создавать новый лог-файл по достижении 2 МБ
Сохранять лог-файл в *.HTML формате
Вести дополнительный лог в журнале приложений Windows
Запускать USB Guard автоматически
Запускать USB Guard в трей-режиме
Отключить USB порты при запуске
Сохранить изменения

СХЕМА «USB GUARD»

ПАК «USB GUARD»





РЕЗУЛЬТАТЫ

1. Рассмотрены и проанализированы возможные способы защиты от атаки BadUSB.
2. Разработано программное обеспечение для контроля подключаемых USB-устройств.
3. Разработана модель программно-аппаратного комплекса для контроля подключаемых USB-устройств с использованием устройств доступных в свободной продаже.