ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ К ВНЕШНЕМУ МОДУЛЮ ЗАЩИТЫ USB ПОРТА ОТ АТАКИ BADUSB И ПРОГРАМЫ ДЛЯ НАСТРОЙКИ КОНФИГУРАЦИИ

Москва 2026

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ 3
1.1 ОБЛАСТЬ ПРИМЕНЕНИЯ 3
1.2 КРАТКОЕ ОПИСАНИЕ ВОЗМОЖНОСТЕЙ 3
1.3 УРОВЕНЬ ПОДГОТОВКИ ПОЛЬЗОВАТЕЛЯ 3
2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ 3
3 ПОДГОТОВКА К НАСТРОЙКЕ 3
4 ПОДГОТОВКА К РАБОТЕ 4
5 ОПИСАНИЕ ОПЕРАЦИЙ 4
6 АВАРИЙНЫЕ СИТУАЦИИ 8

1 ВВЕДЕНИЕ

1.1 ОБЛАСТЬ ПРИМЕНЕНИЯ

Требования настоящего документа применяются перед тестированием, эксплуатацией или настройкой устройства.

1.2 КРАТКОЕ ОПИСАНИЕ ВОЗМОЖНОСТЕЙ

Устройство служит для внешней защиты от атак с BadUSB на USB-порт, ограничивает доступ к USB-периферии и разрешает активацию согласно настраиваемому списку разрешённых классов устройств или пары код производителя и код устройства, блокирует сигнальные линии в случае подключения BadUSB, при этом устройство постоянно подключено к USB-порту, не мешая его работе, что даёт постоянную защиту.

1.3 УРОВЕНЬ ПОДГОТОВКИ ПОЛЬЗОВАТЕЛЯ

Для эксплуатации пользователь должен обладать знаниями работы с внешними устройствами с USB 2.0.

Для настройки должен обладать знаниями работы с внешними устройствами с USB 2.0, электронными вычислительными машинами.

2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

Устройство предназначено для постоянной защиты порта с USB 2.0 от атак BadUSB или для фильтрации доступа периферийных устройств.

Работа с устройством возможно всегда, когда есть подключение устройства к USB 2.0 type A порту и подключенным к нему внешнему USB устройству.

3 ПОДГОТОВКА К НАСТРОЙКЕ

Для подготовки к настройке выполните действия в следующем порядке:

1. Подключите к ЭВМ к интернету
2. Установите приложение настройки конфигурации по ссылке:

https://github.com/MicroZerg/BadUSBGuard.git

3. Подготовьте список доверенных VID и PID устройств и dClass

4 ПОДГОТОВКА К РАБОТЕ

Для подготовки к работе выполните действия в следующем порядке:

1. Подключите к устройству-хосту защитное устройство
2. Проверьте заземление устройства-хоста
3. Проверьте работу устройства с помощью теста

Для проверки подключите разрешённое периферийное устройство к защитному устройству. При выполнении своих функций внешним устройством USB работа исправна, иначе перепроверьте настройки защитного устройства и параметры разрешённого устройства, если функции не выполняются, то оно повреждено.

5 ОПИСАНИЕ ОПЕРАЦИЙ

Устройство выполняет функцию длительной защиты устройств с USB type A от атак BadUSB, не мешая его работе и задачи, приведенные ниже:

Задача: «Работа разрешённого внешнего устройства через устройство защиты с USB type A»

1. Операция: Подключение внешнего устройства через устройство защиты с USB 2.0 type A.
2. Условия, при соблюдении которых возможно выполнение операции:

   На устройстве хосте включены USB порты.

3. Подготовительные действия:

   На ЭВМ хоста необходимо выполнить подключение устройства защиты к USB 2.0 type A.

Предварительно настроить конфигурацию защитного устройства, если оно уже не было настроено.

4. Основные действия в требуемой последовательности:

   - Подключение внешнего USB устройства к устройству защиты.
   - Проверка корректности работы внешнего устройства.

5. Заключительные действия:

   Не требуются.

6. Ресурсы, расходуемые на операцию:

   5-10 секунд.

Задача: «Защита устройства хоста от BadUSB или запрещённого устройства»

1. Операция: Подключение BadUSB или запрещённого устройства через устройство защиты.
2. Условия, при соблюдении которых возможно выполнение операции:

   На устройстве хосте включены USB порты.

3. Подготовительные действия:

   На ЭВМ хоста необходимо выполнить подключение устройства защиты к USB 2.0 type A.

4. Основные действия в требуемой последовательности:

   - Подключение BadUSB или запрещённого устройства к устройству защиты.

5. Заключительные действия:

Изъятие BadUSB или запрещённого устройства после срабатывания защиты.

6. Ресурсы, расходуемые на операцию:

   5-10 секунд.

Задача: «Настройка устройства защиты»

1. Операция: Настройка конфигурации устройства защиты с помощью электронной вычислительной машины.
2. Условия, при соблюдении которых возможно выполнение операции:

   На устройстве хосте включены USB порты.

   Установлено приложение для настройки конфигурации.

   Желательно электронная вычислительная машина должна иметь доступ в интернет.

3. Подготовительные действия:

   На ЭВМ хоста необходимо выполнить подключение устройства защиты через контроллер.

   Запустить приложение настройки конфигурации.

   Если приложение запускается впервые проверить наличие подключения к интернету.

4. Основные действия в требуемой последовательности:

   a. При небольшом числе изменений разрешённых VID и PID или dClass:

      - Выбрать порт, к которому подключено устройство.

- Для добавления вписать в подписанные поля, доверенные VID и PID устройства и нажать кнопку Save, повторить несколько раз при нескольких устройствах.
- Для удаления выбрать VID и PID устройства и нажать кнопку Delete, повторить несколько раз при нескольких устройствах.
- Для добавления вписать в подписанное поле, доверенный dClass устройств и нажать кнопку Save, повторить несколько раз при нескольких dClass.
- Для удаления выбрать dClass устройств и нажать кнопку Delete, повторить несколько раз при нескольких dClass.
- Нажать кнопку Load.
- Ожидайте до закрытия окна командной строки.

b. При большом числе изменений разрешённых VID и PID или dClass:

- Открыть файл Configuration.txt
- Для добавления VID и PID вписать в первую строку список доверенных VID и PID устройств в формате:

  [['0000', '0000'], ['ffff', 'ffff']]
- Для добавления dClass вписать в вторую строку список доверенных dClass в формате:

  ['00', '08', 'ff']
- Для удаления VID и PID удалить из первой строки блоки VID и PID устройств сохраняя формат строки:

  [['0000', '0000'], ['ffff', 'ffff']]

- Для удаления dClass удалить из второй строки, доверенные dClass сохраняя формат строки:

  ['00', '08', 'ff']

- Сохранить изменения в файле.
- Перезапустить приложение настройки.
- Выбрать порт, к которому подключено устройство.
- Нажать кнопку Load.
- Ожидайте до закрытия окна командной строки.

5. Заключительные действия:

   Изъятие устройства защиты и проверка корректности работы.

6. Ресурсы, расходуемые на операцию:

   20-30 секунд.

6 АВАРИЙНЫЕ СИТУАЦИИ

При подключении USB killer-а к устройству защиты, оно защищает от атаки USB killer, но при этом сгорает мультиплексор и может сгореть контроллер, что прекращает его работу до замены компонентов и может привести к возгоранию.