

# Убить USB-киллера

С. Пескова<sup>1</sup>

УДК 621.315 | ВАК 05.27.01

Предлагается эффективное решение многоуровневой защиты, которое могут использовать разработчики мобильного оборудования с USB-интерфейсом на борту для предотвращения вредоносных USB-атак.

С о времен дебюта (примерно с 1995 г.) и по сей день USB-порт облегчает соединение между компьютерной периферией и персональным компьютером, мобильным телефоном, смартфоном, планшетом и т. д. Ученых давно волнуют вопросы безопасности и рисков, связанных с подключением USB-дисков к компьютеру, даже если эти устройства заслуживают доверия. В случаях, когда угроза заражения компьютера вирусом решена для пользователя на высоком уровне, остается риск «убить» оборудование простым подключением USB-накопителя, если это USB-killer.

Круг жертв такого устройства не ограничивается компьютерами, ноутбуками или планшетами. Оно способно повредить любой прибор с USB Host интерфейсом на борту, например, осциллографы, мультиметры, ТВ, роутеры и т. д. Несмотря на очевидные вредоносные свойства, USB-killer не осуждают пользователи, регулярно появляются новые версии и «апгрейды», смертоносную флешку легко купить на Aliexpress или в других доступных интернет-магазинах.

В данной статье объясняется, как работает и какие повреждения USB-killer может нанести USB-порту. Предлагается эффективное решение многоуровневой защиты, которое могут использовать разработчики мобильного оборудования за пределами применяемых сегодня минимальных стандартов.

## USB-KILLER – ЧТО ЭТО?

USB-убийца – это проблема разработчиков по защите USB-порта от пары сотен вольт и пары сотен ампер. USB-убийца – вредоносный USB flash-носитель, который сначала заряжается через USB-шину (Vbus), а потом вызывает бросок мощности между 220/240 В переменного тока и импульсы тока более 175 А в USB-канал данных (рис. 1). То есть при подключении к порту запускается преобразователь напряжения,

который заряжает внутренние конденсаторы флешки до 220 В. Затем преобразователь выключается, и накопленная энергия подается на сигнальные линии USB-интерфейса (рис. 2).

Такой мощный выброс делается повторными циклами с намерением повредить что угодно, не выдерживающее подобных скачков. После разрядки конденсаторов цикл повторяется, преобразователь снова заряжает конденсаторы. Вредоносный диск может вызвать широкий круг проблем – от поломки порта до неконтролируемых термоэффектов. Поскольку сегодня многие мобильные устройства стоят недешево или применяются для решения критических задач, требуется обеспечить их защиту от подобных USB-угроз.

Стандартная защита USB-порта хорошо известна. Обычная практика – защита USB-линий данных с помощью ESD-компонентов, что соответствует стандарту IEC61000-4-2(ESD). К сожалению, USB-убийца может воспользоваться этим известным уровнем защиты в своих интересах.

Разработанный для «обхода» традиционных способов защиты USB-линий данных USB-убийца генерирует слишком большую мощность, которую не выдерживают стандартные ESD-компоненты защиты. После первой пары импульсов последующие выбросы напряжения повреждают любые электронные компоненты на своем пути за пределами USB-контроллера, и в некоторых случаях приводят к неконтролируемым термодарам.

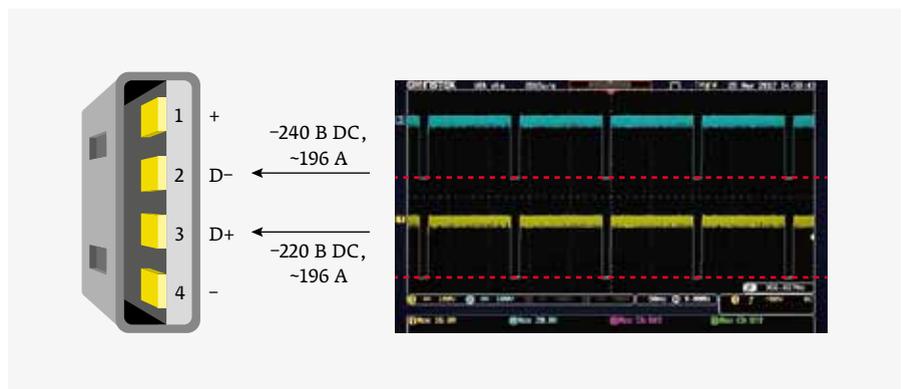


Рис. 1. Осциллограмма сигнала вредоносного USB-накопителя

<sup>1</sup> Платан, начальник отдела маркетинга, Svetlana@platan.ru.



Рис. 2. USB-флешка – убийца

### ЭФФЕКТИВНАЯ СИСТЕМА ЗАЩИТЫ

Среди широкого круга компонентов защиты важно найти правильное надежное решение для защиты от USB-убийц. После тестирования и изучения параметров выбросов USB вредоносных носителей и особенностей повреждения электронных плат разработчики компании Vougrns пришли к выводу о необходимости использования комбинированной многоуровневой системы защиты, в которую входят TVS-диоды, TBU-устройства высокоскоростной защиты и газовые разрядники.

Традиционная схема безопасности USB-порта, где применяются TVS-диоды для защиты от статики и PPTC-компоненты для защиты от превышений по току и/или обратной полярности подключения, представлена на рис. 3. Для создания эффективного барьера от бросков

USB-напителя необходимо добавить в схему TBU-компонент и газовый разрядник.

TBU-устройства как ограничители по току обеспечивают эффективную защиту от удара молнии, индукционных наводок, пересечения питания или других выбросов. Производимые по MOSFET-технологии TBU-компоненты, размещенные последовательно сигнальной линии, контролируют ток, протекающий в линии. Если ток превышает предустановленный уровень, устройство срабатывает, создавая надежный барьер высокому напряжению и току. TBU-защита действует молниеносно – через 1 мс. В режиме блокировочной защиты компонент ограничивает ток до уровня около 1 мА и блокирует напряжение до максимального рабочего напряжения компонента. После выброса TBU-устройство восстанавливается, если напряжение падает ниже уровня  $V_{reset}$ , и полностью возобновляет защитные функции, когда параметры сигнальной линии возвращаются к норме.

Слагаемые эффективности TBU-защиты в случае с вредоносными USB-напителями:

- последовательное подключение компонентов;
- срабатывание при заданном уровне тока;
- блокировка напряжения до 850 В, возможность простого координирования;
- обеспечение превосходной защиты со скоростью менее 1 мкс;
- не повышает емкость сигнальной линии;
- чрезвычайно низкая потребляемая мощность;
- самовосстановление;
- очень широкая полоса пропускания;
- миниатюрные размеры компонентов в DFN-корпусах.

Применение газового разрядника с низкой емкостью (менее 1 пФ) делает это решение аналогичным делителю

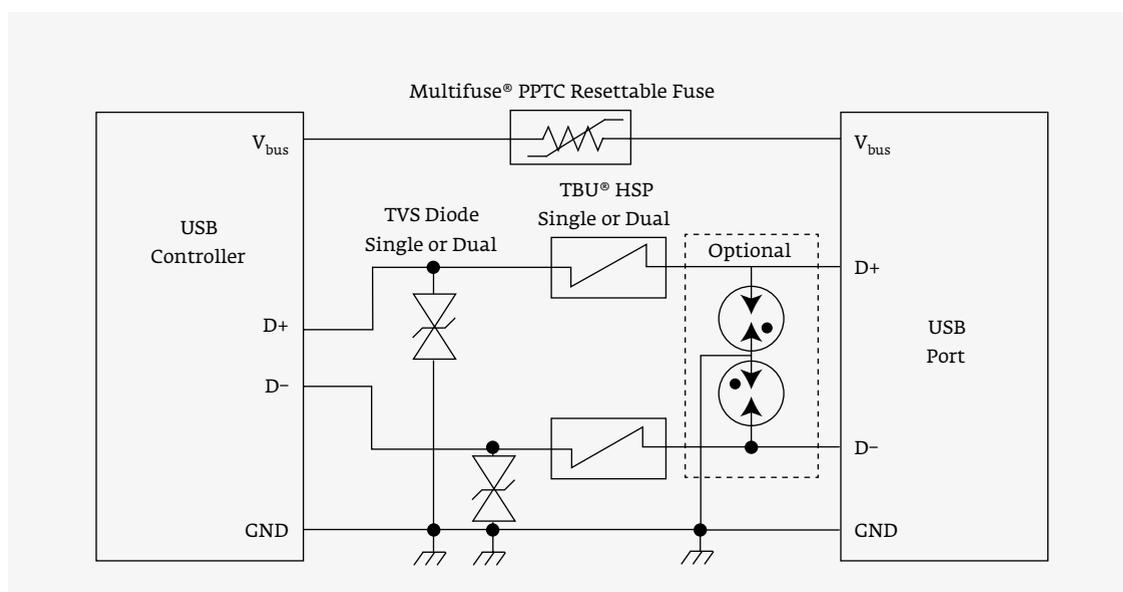
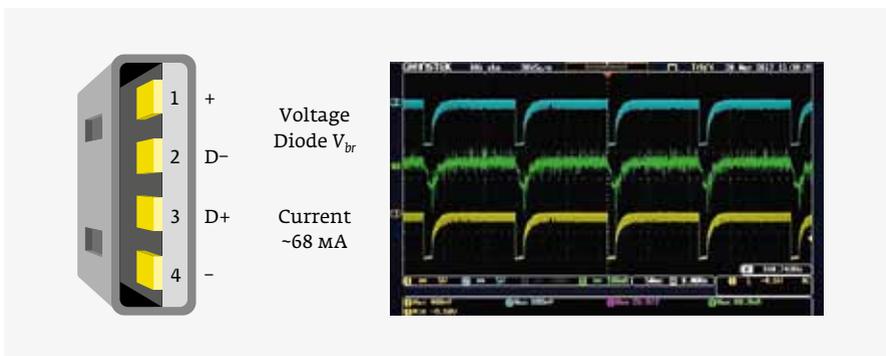


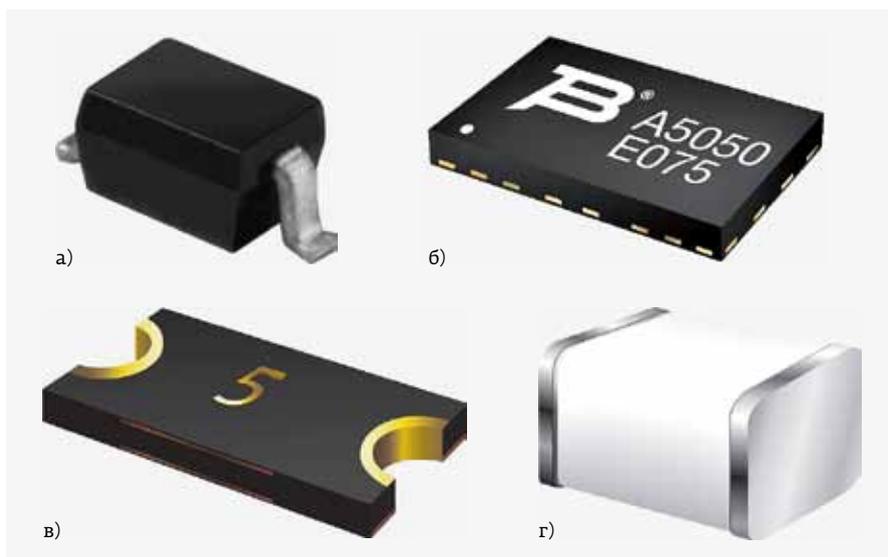
Рис. 3. Решение для защиты USB-порта от перенапряжения



**Рис. 4.** Осциллограмма сигнала от USB-убийцы после применения компонентов защиты  $V_{br}$ ns

напряжения. Разрядник номиналом более 2 кА – дополнительное устройство для разрядки емкости USB-накопителя на этапе нескольких первых пар выбросов.

Газовый разрядник работает по газо-физическому принципу как высокоэффективный компонент разрядки дугового электрического сигнала. Разрядник поддерживает высокий импеданс до тех пор, пока напряжение не превышает уровень его напряжения пробоя. В этот момент газ внутри корпуса ионизируется и становится проводником за несколько микросекунд. В состоянии пробоя разрядник отличается низким импедансом, что приводит к низкому уровню рабочего напряжения. Компонент эффективно ограничивает высокое напряжение до низкого уровня и шунтирует протекающий ток. После завершения выброса напряжение системы возвращается на исходный уровень, и разрядник переходит в состояние высокого импеданса.



**Рис. 5.** Компоненты защиты: а – TVS-диод, б – TBU-защита, в – самовосстанавливающийся предохранитель, г – газовый разрядник

Результаты тестирования данной схемы при использовании только TVS- и TBU-компонентов показаны на рис. 4. Здесь видно значительное уменьшение напряжения и тока. В этом случае напряжение снижается до уровня  $V_{br}$  TVS-диода, а ток уменьшается до управляемого уровня 68 мА. Следует подчеркнуть, что повторяющиеся импульсы прекратятся только в момент полной разрядки конденсаторов.

Приведем список компонентов, которые можно использовать для разработки защиты разного уровня,

сами компоненты показаны на рис. 5.

#### Вариант 1 (четыре компонента):

- два TVS-диода CDSOD323-T05LC (1 пФ), по одному на линии данных D+ и D-;
- два TBU высокоскоростных устройства защиты TBU-CA040-050-WH, по одному на линии данных D+ и D-.

#### Вариант 2 (семь компонентов):

- один Multifuse PPTC модели MF-NSMF075-2 (на шину  $V_{bus}$ );
- два TVS-диода CDSOD323-T05LC (1 пФ), по одному на линии данных D+ и D-;
- два TBU высокоскоростных устройства защиты TBU-CA065-050-WH, по одному на линии данных D+ и D-;
- два SMT газовых разрядника 2051-09-SM, по одному на линии данных D+ и D- для разрядки емкостного банка.

Выбор решения зависит от свободного пространства печатной платы и требуемого уровня защиты. Основное различие двух вариантов заключается в использовании газового разрядника. При подключении вредоносного USB-устройства циклы блокировки будут продолжаться до тех пор, пока емкость не разрядится полностью, что может занять некоторое время. При использовании второго варианта с газовым разрядником разрядка емкости произойдет уже в первую пару циклов выбросов. Многоуровневый подход к системе безопасности обеспечивает разработчикам мобильного оборудования эффективное решение для защиты от вредоносных USB-атак. ●