Беспроводной кейлоггер

сделай сам!

Введение

Известно ли Вам понятие "аппаратный кейлоггер"? Аппаратный кейлоггер - это идеальное решение, служащее для мониторинга активности пользователя компьютера, с ничтожным риском обнаружения. Аппаратный кейлоггер - это в 100% электронное устройство, а, значит, оно не требует доступа к операционной системе, не оставляет никаких следов, а программное обеспечение не в состоянии обнаружить устройства такого типа. Концепция аппаратного кейлоггера, однако, имеет один недостаток: чтобы получить перехваченные данные, нужно иметь физический доступ к устройству. Эта проблема, наконец, нашла решение: беспроводной кейлоггер.

KeeLog в прошлом уже опубликовал один проект аппаратного кейлоггера PS/2 типа Open Source. Сейчас мы делаем это вновь с проектом беспроводного кейлоггера, предназначенного для самостоятельного монтажа. Этот проект можно использовать как в личных, так и в коммерческих целях, со следующими ограничениями:

1. Все материалы, помещённые на этом сайте, являются интеллектуальной собственностью фирмы KeeLog, и их использование означает акцептацию нижеприведённых условий и общего Соглашения об использовании сайта.
2. Этого проект беспроводного кейлоггера опубликован "как есть", со всеми недостатками и без всякой гарантии.

Беспроводной кейлоггер не должен использоваться для незаконного перехвата чужих данных, в частности, паролей, банковских данных, конфиденциальной корреспонденции и т.п. В большинстве стран это является нарушением закона.

Беспроводной кейлоггер состоит из двух основных частей: передатчика и приёмника. Реальное считывание клавиш происходит в передатчике, который является, по сути, аппаратным кейлоггером PS/2, со встроенным аудио-модулем 2.4 GHz. Перехваченные данные с клавиатуры не архивируются в памяти, а передаются в реальном времени по радиосвязи. Приёмник, с другой стороны, является беспроводным накопительным устройством с интерфейсом USB. Все данные, полученные с передатчика, высылаются с компьютера через USB. С программной точки зрения эти данные доступны через виртуальный порт COM, что позволяет производить их визуализацию с помощью любого клиента терминала.

Беспроводной кейлоггер - блочная схема

Вся система действует в реальном времени, а, следовательно, текст, который пишется на удалённом компьютере, сразу же виден со стороны приёмника. Система имеет максимальный радиус действия около 50 метров. Это соответствует эффективному радиусу действия около 20 метров через 2-4 стены, в зависимости от их толщины.

Беспроводной кейлоггер - передатчик

Беспроводной кейлоггер - приёмник

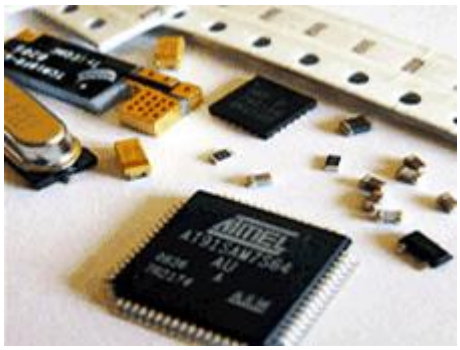
Как передатчик, так и приёмник опираются на одну и ту же принципиальную схему и печатную схему. У обоих одни и те же габариты, и они предназначены для крепления на коротких удлинителях PS/2 и USB. Рекомендуется использовать корпус от фильтров типа EMC, что приведёт к тому, что устройство в целом будет напоминать адаптер или удлинитель.

Компоненты

В этой статье описан весь процесс монтажа беспроводного кейлоггера. В зависимости от навыков Вы можете создать собственный беспроводной кейлоггер с нуля, или заказать у нас компоненты. Мы может поставить комплект компонентов вместе с запрограммированными микроконтроллерами и стандартными корпусами (см. фото), или полностью смонтированный и тестированный комплект устройств. Перейти в секцию Комплекты, чтобы узнать больше подробностей.

Если Вы решили создать свой собственный беспроводной кейлоггер, Вы должны быть знакомы с основами электроники и пайки, лучше всего - с технологией поверхностного монтажа (SMT). Наиболее простая опция - это заказ комплекта компонентов у нас и самостоятельное выполнение пайки, прокладки кабелей и финального монтажа. Для этого нужно иметь паяльник с регулировкой температуры и довольно хорошие навыки в пайке. Если Вы решили запроектировать и выполнить печатные схемы самостоятельно, это потребует большего опыта и соответствующего оборудования.

В нижеприведённой таблице представлен перечень компонентов (BOM), необходимых для выполнения одной штуки передатчика или приёмника. Дополнительный удлинитель PS/2 необходим для передатчика, а кабель USB с коннектором типа A требуется для приёмника.



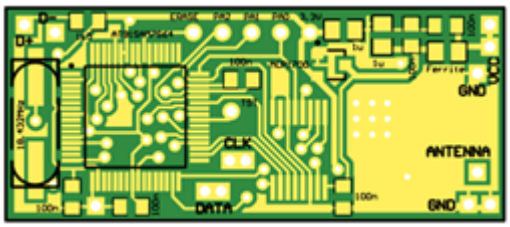
Перечень электронных компонентов

Кабели, корпус, а также печатные схемы

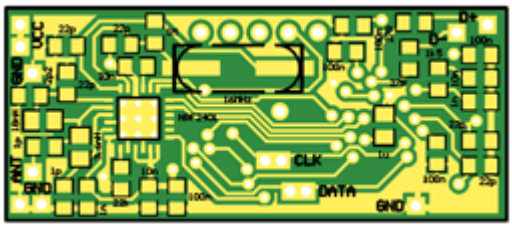
Указатель	Описание	Корпус	Количество
U1	Микроконтроллер AT91SAM7S64	TQFP64	1
U2	Трансивер nRF24□1	QFN24	1
U3	Стабилизатор MCP1700T-330	SOT-23	□
Q1	Кварцевый генератор 18.432 MHz	HC-49 SMD	1
Q2	Кварцевый генератор 16 MHz	HC-49 SMD	1
R1, R2	Резистор 1.5 kΩ	0805	2
R3, R4	Резистор 27 Ω	0805	2
R5	Резистор 1 MΩ	0805	1
R6	Резистор 22 kΩ	0805	1
C1, C27	Конденсатор 10 nF	0805	2
C2, C28	Конденсатор 1 nF	0805	2
C3, C4, C6, C7, C8	Конденсатор 22 pF	0805	5
C5	Конденсатор 33 nF	0805	1
C9	Конденсатор 2.2 pF	0805	1
C10, C11	Конденсатор 1 pF	0805	2
C12, C22, C23, C24, C25, C26, C32, C33, C34, C42, C43	Конденсатор 100 nF	0805	11
C21, C31, C41	Конденсатор 1 μF	0805	3
L1	Дроссель	□805	1
L2	Катушка 3.6 nH	0805	1
L3	Катушка 18 nH	0805	1

Беспроводной кейлоггер - перечень компонентов

Как для передатчика, так и для приёмника используется одна и та же печатная схема и один и тот же комплект компонентов (отличаются они системой кабелей и прошивкой). Микроконтроллер Atmel AT91SAM7S64 и радио-трансивер nRF2401 - это ключевые компоненты электронной схемы. Оба они нуждаются в кварцевых осцилляторах для правильной работы. Кроме стабилизатора MCP1700, все прочие компоненты пассивны (резисторы, конденсаторы и несколько катушек). Обычный отрезок проволоки рекомендуется в качестве дипольной антенны. Двусторонняя двухслойная печатная схема показана на рисунках ниже.

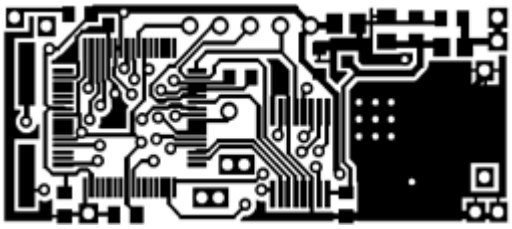


Расклад печатной схемы - верхняя сторона

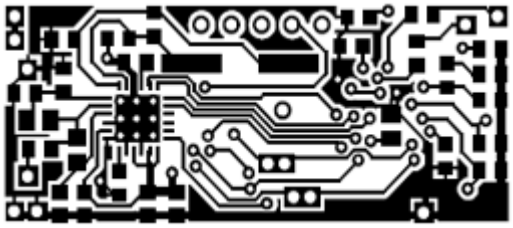


Расклад печатной схемы - нижняя сторона

Если Вы располагаете достаточным опытом, чтобы выполнить печатные схемы самостоятельно, Вы можете воспользоваться комплектом масок в масштабе 1:1, доступных ниже. В проекте использован слоистый пластик типа FR4 толщиной 1 мм.



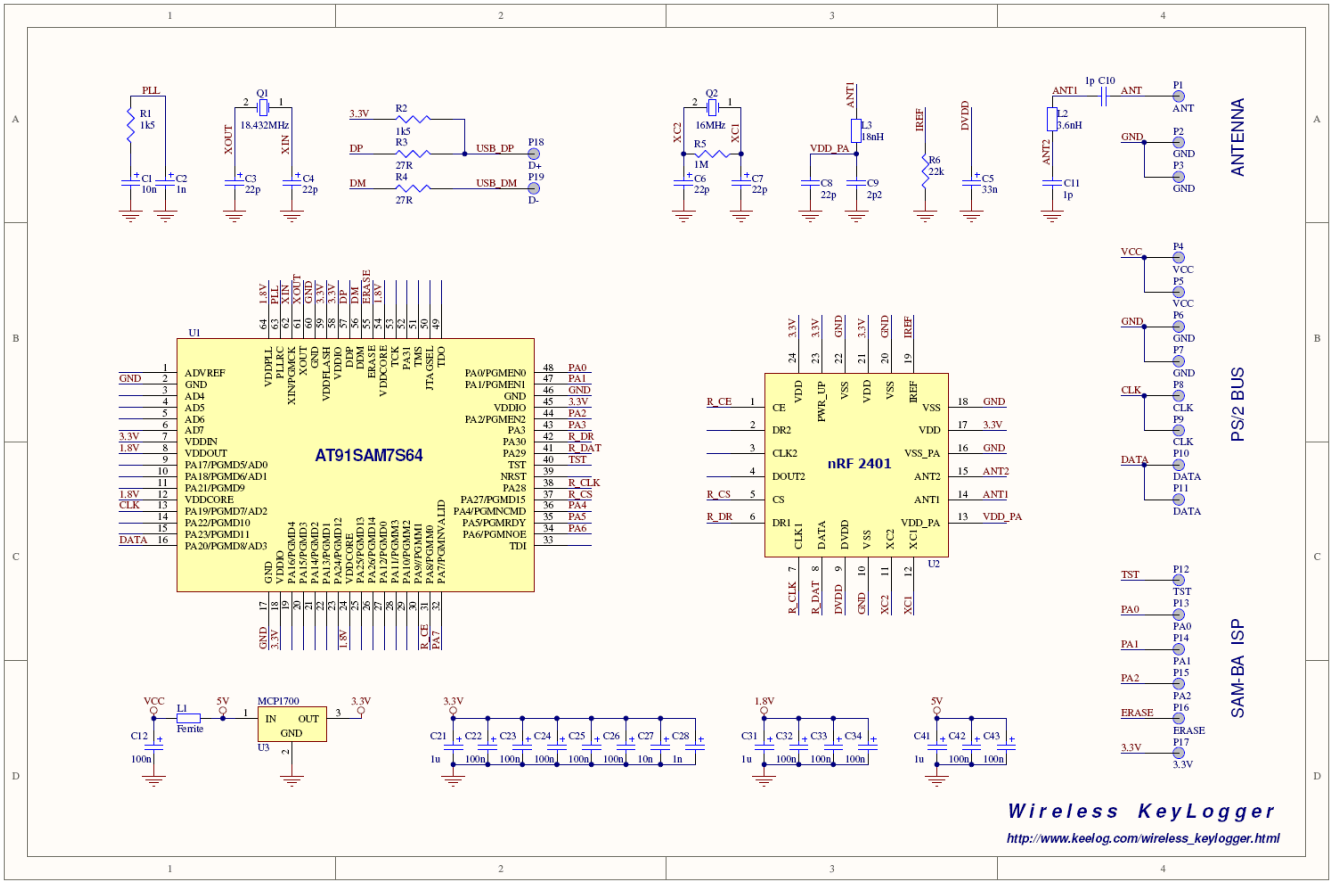
Маска для печатной схемы - верхняя сторона



Маска для печатной схемы - нижняя сторона

Монтаж

Схема беспроводного кейлоггера состоит из двух главных компонентов: микроконтроллера AT91SAM7S64 и трансивера nRF2401. Сопутствующие им пассивные элементы - это, в основном, осциллятор и высокочастотные схемы RF. Вся схема питается напряжением 3.3V, генерированным стабилизатором MCP1700 и фильтровальным блоком конденсаторов. Входное питание поступает непосредственно с магистрали PS/2 (передатчик), или USB (приёмник). Если у Вас уже есть смонтированные печатные схемы, перейдите к секции Система кабелей. Если Вы решились на самостоятельный монтаж, нижеприведённые указания и принципиальная схема Вам пригодятся.



Беспроводной кейлоггер - принципиальная схема

Для пайки используйте паяльник с тонким наконечником (обычно менее 0,5 мм) и паяльную пасту (например, RMA7). Следите за тем, чтобы не перегреть элементы во время пайки. Монтаж начинайте от трансивера nRF2401 в связи со сложным типом корпуса. Затем переходите к микроконтроллеру AT91SAM7S64 и стабилизатору MCP1700. Следите, чтобы пин номер 1 на корпусе совпадал с первым пином на печатной схеме. В конце припаять все дополнительные схемы: кварцевые генераторы, резисторы, конденсаторы и катушки. Антенну нужно оставить на самый конец. Можно использовать антенну с полосой частот ISM 2.4 GHz, или выполнить простую четвертьволновую дипольную антенну из кусочка проволоки. Оптимальная длина - 3,125 см (1,23").

как на помещённых ниже снимках.

Смонтированная печатная схема - верхняя сторона с микроконтроллером

Смонтированная печатная схема - нижняя сторона с трансивером

После монтажа печатных схем нужно выполнить систему кабелей. Кроме прошивки, это то, чем передатчик отличается от приёмника. Передатчик должен быть соединён параллельно с магистралью PS/2. Печатная схема передатчика имеет пэды, позволяющие припаять кабели, ведущие как к компьютеру, так и к клавиатуре. Приёмник же должен иметь стандартное подключение к порту USB. На помещённых ниже снимках показано, как выполнить все соединения.

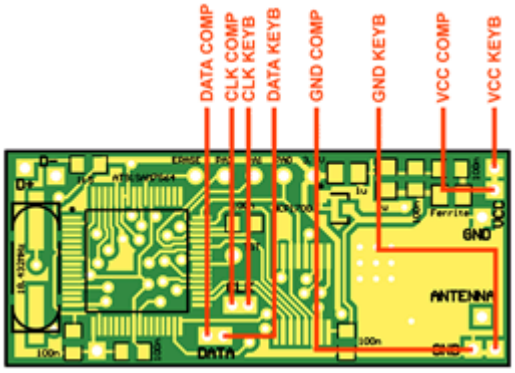


Схема системы кабелей PS/2 для передатчика

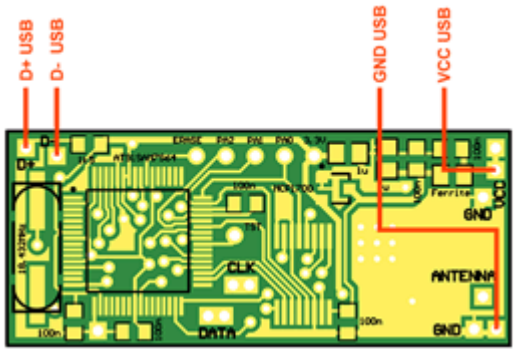
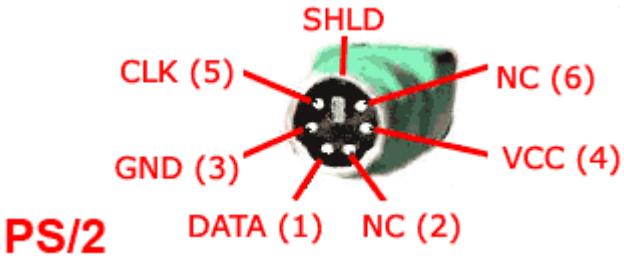


Схема системы кабелей USB для приёмника

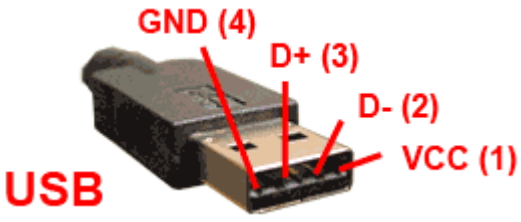
Используйте удлинители PS/2 и USB, перережьте их, снимите изоляцию с сигнальных линий. Вещь, которая может создать некоторые проблемы - это приписывание кабелей к отдельным сигналам. Некоторые кабели PS/2 и USB имеют стандартные цвета, но доверять этому очень рискованно. Рекомендуется применить тестер короткого замыкания или омметр, чтобы узнать, какой кабель соответствует какой сигнальной линии. Нижеприведённые схемы могут в этом помочь.

Сигнал	Описание	Разъём PS/2	Комментарий
VCC	Питание +5V	4	должны быть подключены к модулю
GND	Заземление питания	3	
CLK	Часы	5	
DATA	Данные	1	
NC	Неиспользуемые линии	2, 6	не используемые модулем, если они имеются, оставить в оригинальном состоянии
SHLD	Экран	-	



Разъём PS/2 (передатчик)

Сигнал	Описание	Разъём USB	Комментарий
VCC	Питание +5V	1	должны быть подключены к модулю
D-	Данные	2	
D+	Данные	3	
GND	Заземление питания	4	
SHLD	Экран	-	не используемые модулем, если они имеются, оставить в оригинальном состоянии



Разъём USB (приёмник)

Если микроконтроллеры, которые Вы применяете, ещё не запрограммированы, сейчас удачный момент, чтобы загрузить прошивку, используя технологию ISP (In-System Programming). Прочитайте раздел Прошивки, чтобы узнать больше подробностей. После выполнения этого шага смонтированные устройства должны выглядеть так, как на помещённых ниже снимках.

Передатчик с системой кабелей PS/2

Приёмник с системой кабелей USB

Перед закрытием корпуса рекомендуем выполнить последний тест. Используйте тестер короткого замыкания или омметр, чтобы измерить активное сопротивление между питанием (VCC) и землёй (GND) как на разъёме USB, так и PS/2. Замыкание означает, что нужно проверить всю схему, в противном случае это может привести к повреждению компьютера. Если всё в порядке, закройте корпус, используя клей - и настала пора для первого включения.

Пуск

После монтажа схемы передатчик-приёмник пора выполнить первый тест. Рекомендуется использовать только один компьютер для тестирования обоих устройств. Сначала нужно выключить компьютер и подключить передатчик между клавиатурой PS/2 и портом PS/2.

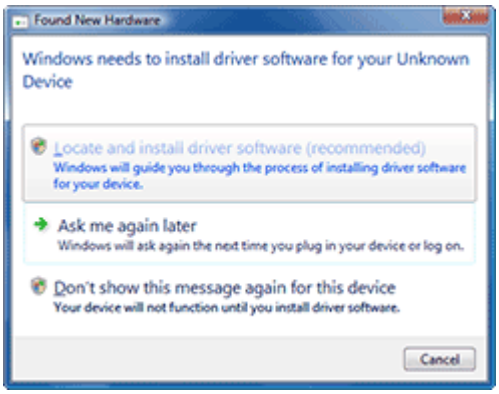
Подключить передатчик к порту PS/2

Подключить клавиатуру PS/2 к передатчику

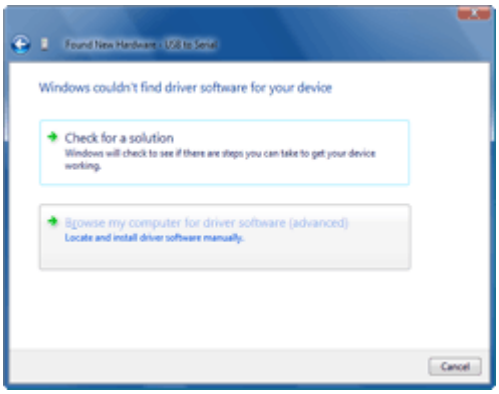
Затем включить компьютер и убедиться в том, что клавиатура PS/2 работает правильно (не должно быть заметно никакого влияния кейлоггера). Затем нужно тестировать приёмник. Перед этим следует скачать файл драйвера KeeLog. Распаковать и сохранить файлы на локальном диске компьютера. Затем подключить приёмник к свободному порту USB (перед этим не требуется выключения компьютера). Убедиться, что позиция приёмника позволяет принимать передачу от передатчика.

Подключить приёмник к свободному порту USB

Когда передатчик подключается в первый раз, появится окно установки драйвера. Точнее, будут использованы драйверы виртуального порта COM, поставляемые с большинством операционных систем, таких как Windows. Но соответствующий файл описания INF должен быть выбран вручную. Когда система спросит о драйверах, перейдите к патчу, где были сохранены файлы драйверов. Нижеприведённые рисунки иллюстрируют весть процесс.

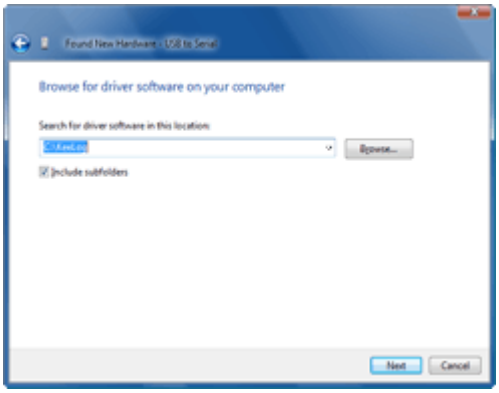


Выбрать локализацию и установку программного обеспечения



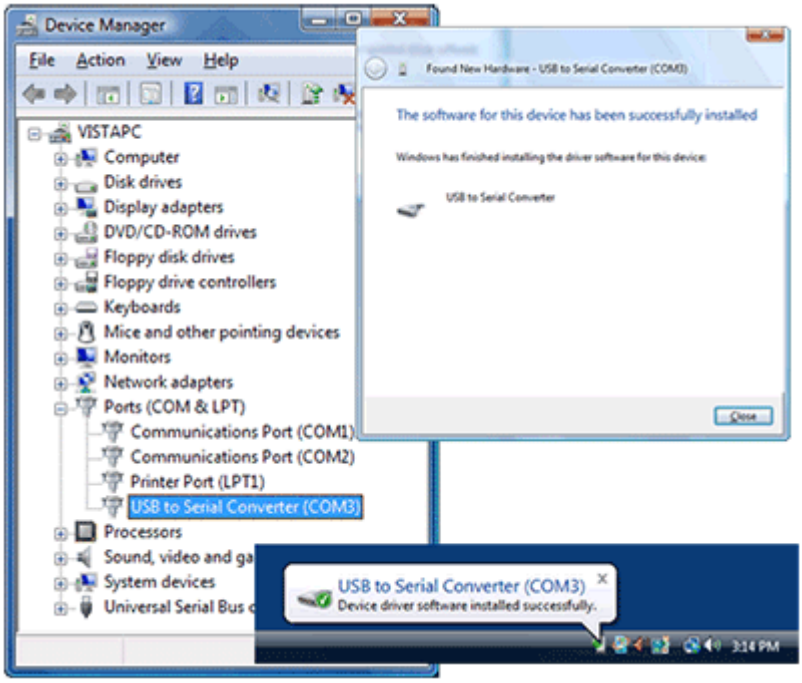
Выбрать локализацию драйвера

Выбрать, чтобы показать опции локализации



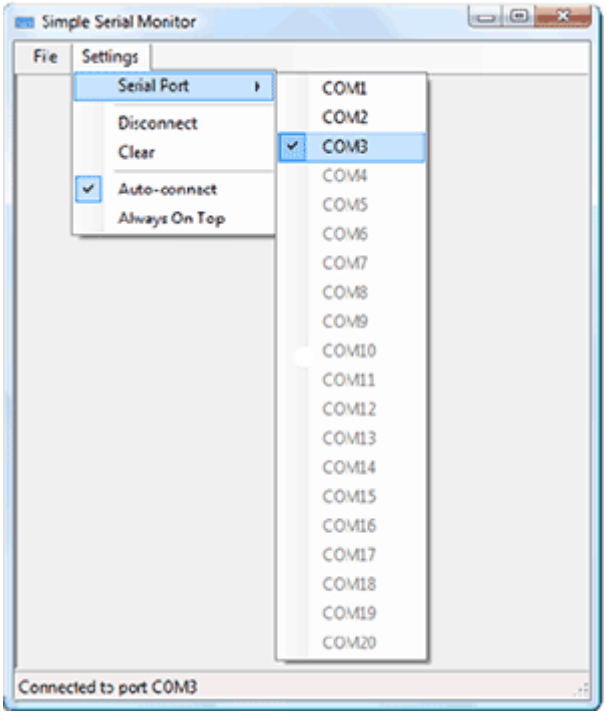
Указать положение файлов драйвера

Если процесс установки закончится успешно, приёмник должен быть виден в Диспетчере устройств как конвертер USB /последовательный порт. Открыть Диспетчер устройств в системе Windows, чтобы проверить, какой последовательный порт приписан к приёмнику.



Приёмник, видимый в Диспетчере устройств

Чтобы начать принимать данные с клавиатуры от передатчика, можно использовать любой клиент терминала, например, Гипертерминал. Рекомендуем использовать нашу бесплатную аппликацию Simple Serial Monitor в связи с её удобством и простотой в использовании.



Simple Serial Monitor (бесплатный клиент терминала, поставляемый KeeLog)

После запуска Simple Serial Monitor (или альтернативной аппликации), помните, чтобы выбрать соответствующий порт COM. Если всё прошло успешно, приёмник тут же начнёт показывать поток клавиш, нажатых на клавиатуре PS/2.

Удалённый компьютер с передатчиком PS/2 *Локальный компьютер с приёмником USB*

Следующим шагом было бы тестирование того же самого на двух разных компьютерах. Убедитесь, что они находятся в радиусе приёма. Если текст появляется в окне терминала, Ваш беспроводной кейлоггер готов к выполнению своей первой реальной задачи. Помните, что нужно использовать это устройство в соответствии с законодательством!

Скачать

Прошивка для микроконтроллера, позволяющая запрограммировать передатчик и приёмник
http://www.keelog.com/files/WirelessKeyloggerFirmware.zip

Драйвер, позволяющий установить приёмник как виртуальный порт COM
http://www.keelog.com/files/UsbToSerial.zip

Бесплатное программное обеспечение, позволяющее принимать перехваченные данные через виртуальный порт COM (аналог аппликации Гипертерминал). Требуется платформа Microsoft .NET Framework.
http://www.keelog.com/files/SimpleSerialMonitor.zip

Программное обеспечение, позволяющее запрограммировать прошивку, применяя SAM-BA
http://www.keelog.com/files/At91Isp.zip

Руководство, как запрограммировать прошивку в микроконтроллер через встроенный bootloader, без использования дополнительного программатора
http://www.keelog.com/files/SambaUserGuide.pdf

Перечень компонентов, использованных для монтажа беспроводного кейлоггера (передатчик и приёмник)
http://www.keelog.com/files/WirelessKeyloggerBom.pdf

Схема кабелей для беспроводного кейлоггера (передатчик и приёмник)
http://www.keelog.com/files/WirelessKeyloggerWiring.pdf

Принципиальная схема беспроводного кейлоггера (передатчик и приёмник)
http://www.keelog.com/files/WirelessKeyloggerSchColor.pdf

Верхняя сторона печатной схемы (передатчик и приёмник)
http://www.keelog.com/files/WirelessKeyloggerPcbTop.pdf

Нижняя сторона печатной схемы (передатчик и приёмник)
http://www.keelog.com/files/WirelessKeyloggerPcbBottom.pdf

Маска для верхней стороны печатной схемы (передатчик и приёмник), масштаб 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskTop.pdf

Маска для нижней стороны печатной схемы (передатчик и приёмник), масштаб 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskBottom.pdf

Прошивка

Прочитайте этот раздел, только если Вам необходимо запрограммировать микроконтроллер AT91SAM7S64 самостоятельно. Если Вы приобрели комплект у нас, мы уже выполнили этот шаг за Вас.

Современные микроконтроллеры, такие как Atmel AT91SAM7S64 имеют плотно упакованные корпуса, что создаёт трудности с подбором традиционного программатора, обслуживающего данный тип микроконтроллера. По этой причине программирование в системе ISP (In-System Programming) в последние годы очень быстро развивается. ISP позволяет сначала смонтировать всю схему, а потом запрограммировать прошивку, нередко используя очень простые инструменты. Микроконтроллер AT91SAM7S64 имеет очень удобное решение ISP, на базе встроенного модуля USB. Он называется SAM-BA (SAM Boot Assistant), и требует только кабеля USB и несколько простых перемычек. Чтобы запустить SAM-BA на беспроводном кейлоггере, сначала скачайте программное обеспечение AT91 ISP. Затем выполните описанные ниже шаги, чтобы загрузить прошивку на модуль передатчика и приёмника.

Шаг 1: Он касается исключительно передатчика. Подготовить кабель USB с разъёмом типа A с одной стороны, и с проводами со снятой изоляцией с другой стороны. Припаять линии USB: VCC, GND, D+, и D- к соответствующим точкам на печатной схеме. Этот шаг не нужен для приёмника, так как он уже имеет подготовленный разъём USB.

Шаг 2: Подготовить несколько коротких проводов, чтобы соединять пины SAM-BA: TST, ERASE, PA2, PA1, PA0, 3.3V. Припаять один конец каждого из проводов к соответствующей точке пайки SAM-BA на обеих платах. Альтернативно Вы можете подготовить специальные перемычки, как показано на рисунках ниже.

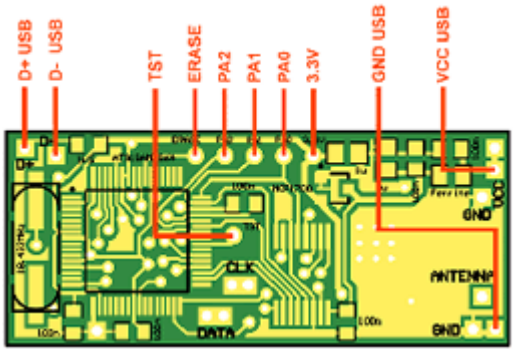
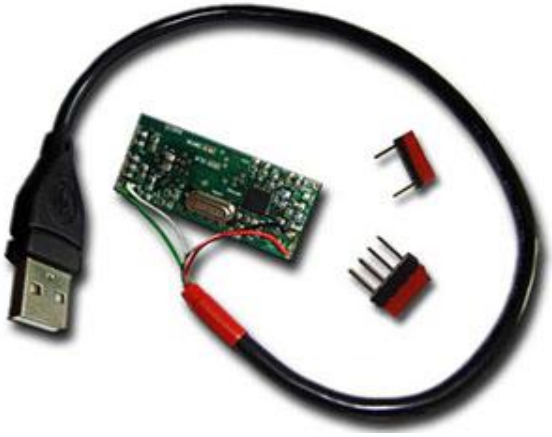


Схема кабелей SAM-BA

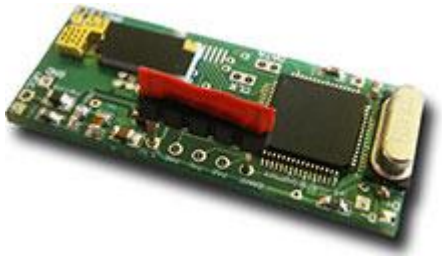
Шаг 3: Установить пакет программного обеспечения AT91 ISP.

Шаг 4: Подключить устройство к свободному порту USB. Сообщение Неизвестное устройство на этом этапе нормально.

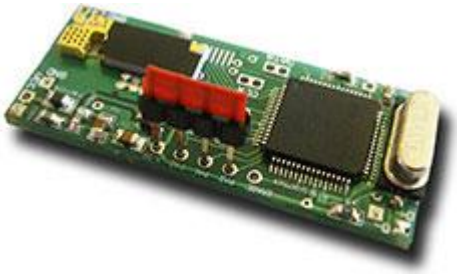
Шаг 5: Присоединить разъём ERASE к 3.3V на момент. Это приведёт к очистке памяти флеш-микроконтроллера.



Кабель USB и перемычки для bootloader SAM-BA



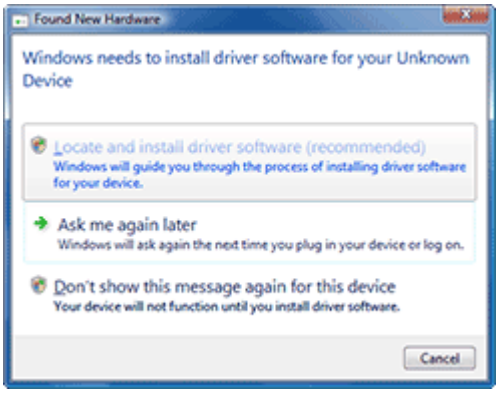
Очистка памяти (ERASE на момент подсоединён к 3.3V)



Активизация bootloader (PA0, PA1, PA2 и TST на момент подсоединены к 3.3V)

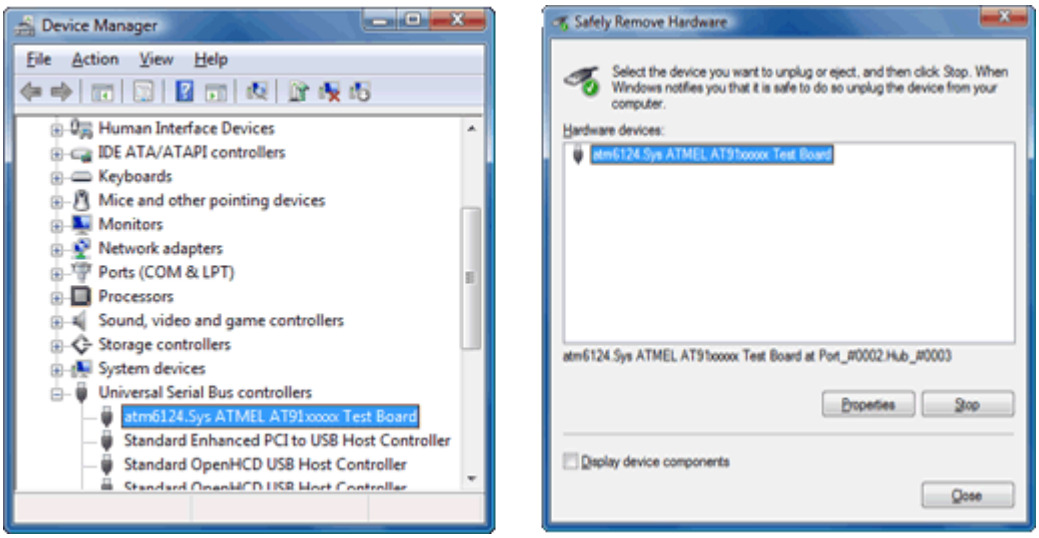
Шаг 6: Отключить устройство от порта USB. Убедиться в том, что разъём ERASE уже не подсоединён к 3.3V. Затем подсоединить комплекс разъёмов PA0, PA1, PA2 и TST к 3.3V. Вновь подключить устройство к порту USB (Неизвестное устройство может снова появиться). Оставить устройство подключённым в течение примерно 10 секунд, а затем отключить его от порта USB. Эта операция должна была активизировать встроенный bootloader SAM-BA.

Шаг 7: Удалить все перемычки или разъёмы и подключить устройство к порту USB. Сообщение Найдено новое оборудование должно появиться. Выполните стандартную процедуру установки и позвольте системе самостоятельно найти драйверы.



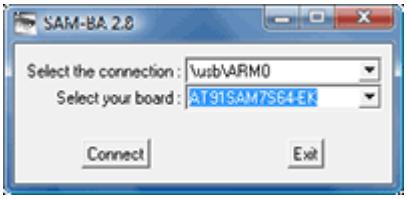
Диалог Найдено новое оборудование

Шаг 8: Открыть Диспетчер устройств, чтобы убедиться в том, что bootloader SAM-BA активизирован.



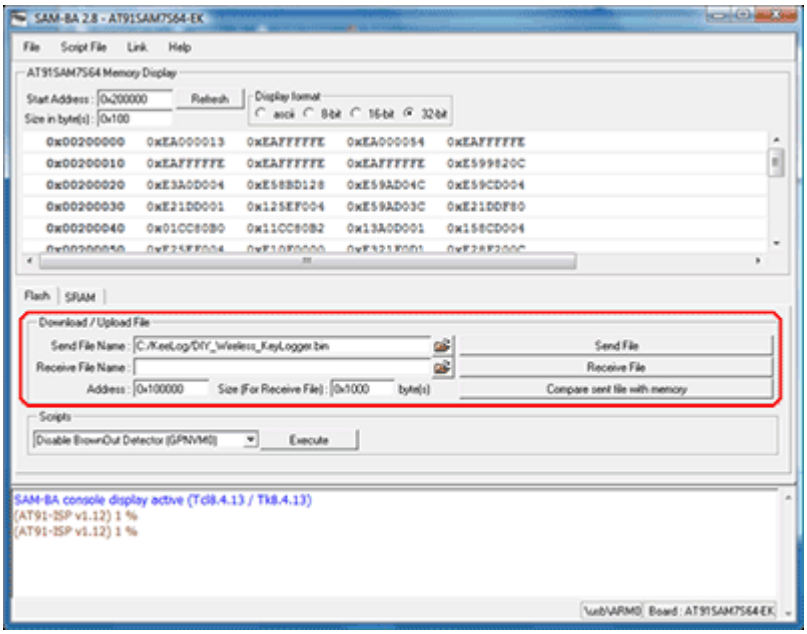
Диспетчер устройств с устройством Atmel AT91

Шаг 9: Запустить аппликацию SAM-BA из пакета программного обеспечения AT91 ISP и выбрать целевую аппаратную платформу AT91SAM7S64-EK.



Выбор аппаратной платформы

Шаг 10: После подключения к аппаратной платформе переключитесь на закладку Flash, выберите соответствующую прошивку для передатчика / приёмника, а затем нажмите Send File. Когда аппликация задаст вопрос, разблокировать ли или заблокировать соответствующие зоны флеш-памяти, следует выбрать Yes. Если это шаг выполнен успешно, это означает, что прошивка успешно загружена в память флеш-микроконтроллера.



Аппликация SAM-BA

Помните, чтобы повторить процедуру SAM-BA как для передатчика, так и для приёмника. После окончания оба устройства готовы к работе.