Надёжное удаление файлов в Windows

Введение

Большинство людей думает, что достаточно отправить файл в «корзину», очистить её, и файл удалён. Это не совсем так. При стирании файла операционная система делает его невидимым для пользователя, а место, занятое на диске этим файлом, помечает как «свободное». Операционная система может использовать это место для записи информации. Могут пройти недели, месяцы, а то и годы, пока файл будет переписан другими данными. До этих пор «удалённый» файл остаётся на диске. Немного усилий, правильные инструменты (компьютерная программа для восстановления данных или специальные приёмы специалиста криминалистической лаборатории), и файл снова жив-здоров. Итак, данные не удаляются сразу и бесповоротно; они остаются на компьютере, пока не понадобится место для других данных.

Если вы хотите удалить файл наверняка, нужно сразу перезаписать его другой информацией. Тогда восстановить данные будет нельзя. Возможно, ваша операционная система уже включает какой-нибудь инструмент, который позволяет записывать поверх удаляемого файла набор «случайных» данных и таким образом защищать конфиденциальность стираемой информации.

Обратите внимание: надёжное удаление данных с твердотельных накопителей (SSD), USB-флешек и карт памяти SD – трудная задача. Рекомендации ниже относятся **только** к обычным жёстким дискам (HDD), но **не** к SSD (которые всё чаще встречаются в современных ноутбуках), USB-флешкам или SD-карточкам.

Причина в том, что в перечисленных выше типах носителей данных применяется технология нивелирования износа.

О стирании данных на SSD-дисках и USB-флешках мы рассказываем в самом конце инструкции.

Для Windows мы рекомендуем программу **BleachBit**. Это бесплатная программа с открытым исходным кодом. Она работает на Windows и Linux и считается гораздо более серьёзным средством, чем встроенный в Windows — **Cipher.exe**.

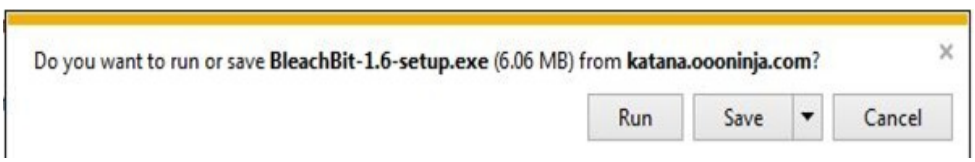
BleachBit можно использовать для быстрого и лёгкого удаления отдельных файлов и для периодического выполнения определённых действий по удалению информации. Можно даже создать свои собственные условия удаления данных.

Получение BleachBit

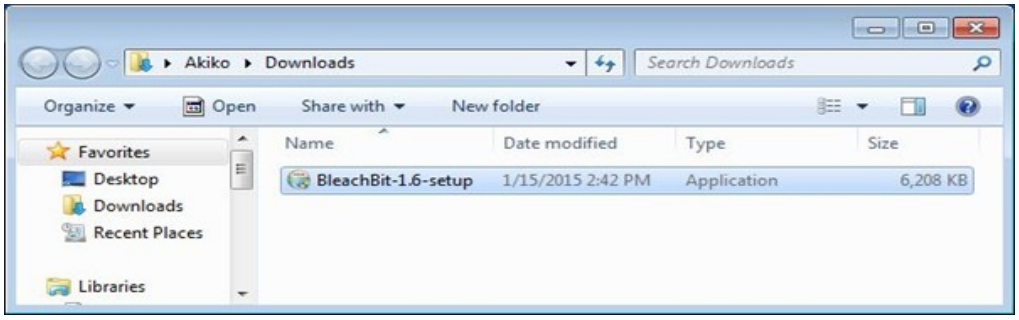
BleachBit для Windows можно найти на странице загрузки BleachBit.

Нажмите ссылку на файл-установщик *BleachBit installer .exe*, вы будете переадресованы на страницу загрузки.

Обычно браузер просит подтвердить загрузку файла. Internet Explorer 11 отображает индикатор в нижней части окна браузера в оранжевой рамке.

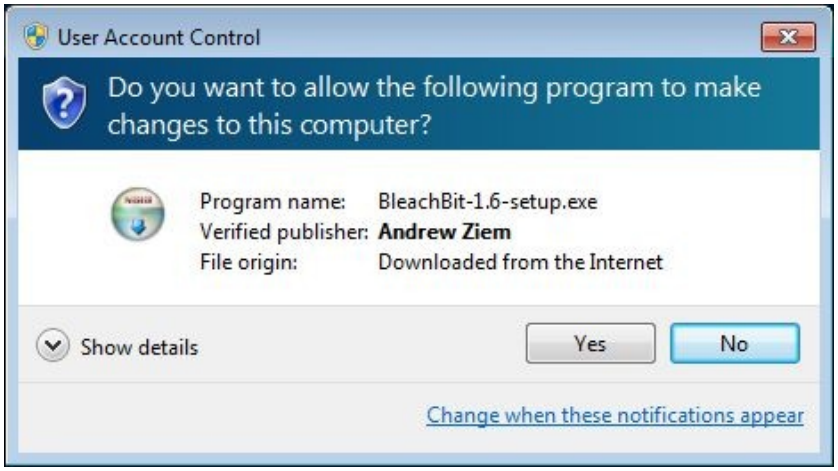


Каким браузером вы бы ни пользовались, лучше сначала сохранить файл, поэтому нажмите кнопку *Save*. По умолчанию большинство браузеров сохраняет загруженные файлы в папке «Downloads».



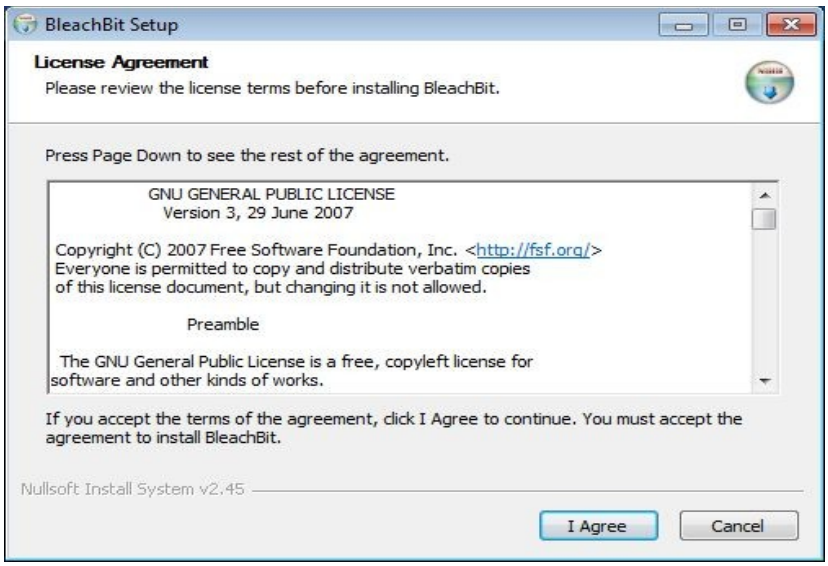
Установка BleachBit

В «Проводнике» Windows дважды нажмите на *BleachBit-1.6-setup*. Нужно подтвердить установку программы. Нажмите кнопку *Yes*.

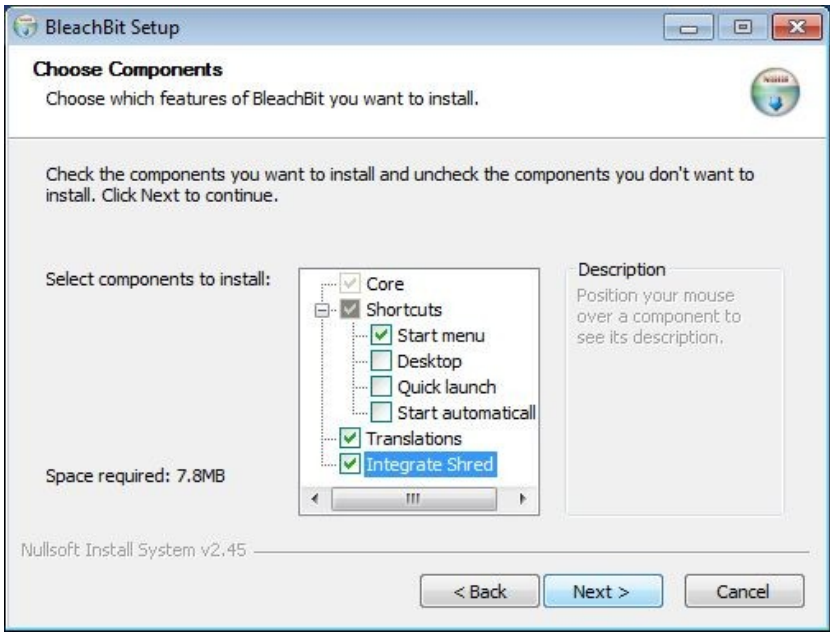


Появится окно с просьбой выбрать язык установки. Сделайте это и нажмите кнопку *OK*.

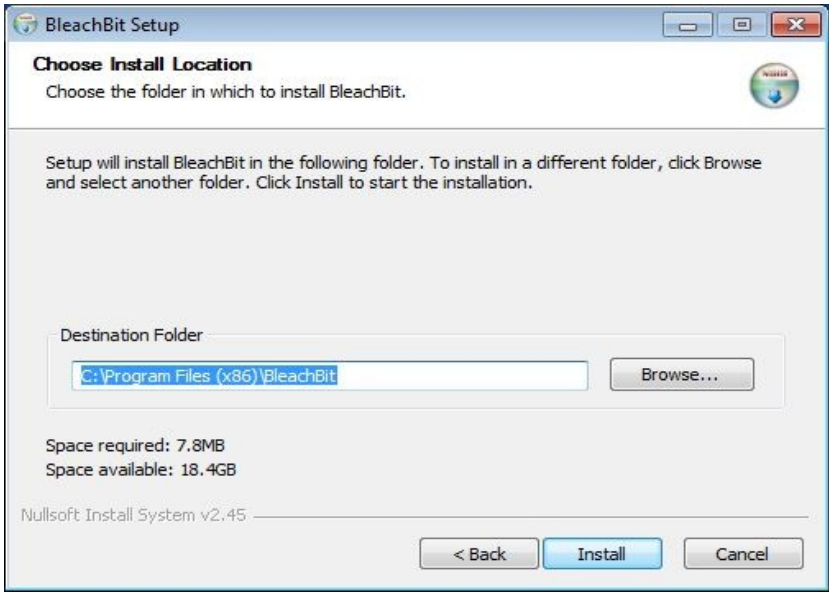
В следующем окне – лицензия GNU General Public License. Примите условия и нажмите кнопку *Next*.



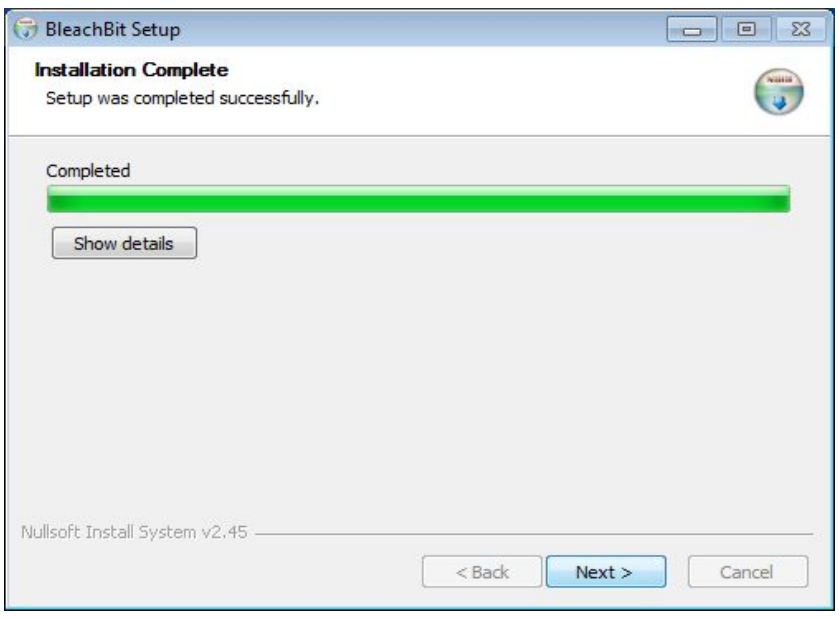
Окно с некоторыми настройками BleachBit. Можно оставить настройки по умолчанию. Советуем снять выделение в поле *Desktop*. Нажмите кнопку *Next*.



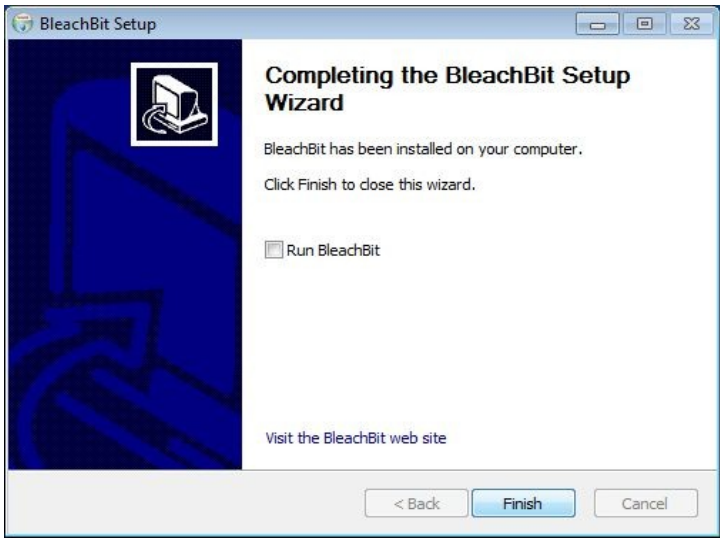
BleachBit снова просит подтвердить намерение установить программу. Нажмите кнопку *Install*.



Наконец, мы видим окно с сообщением об успешной установке. Нажмите кнопку *Next*.



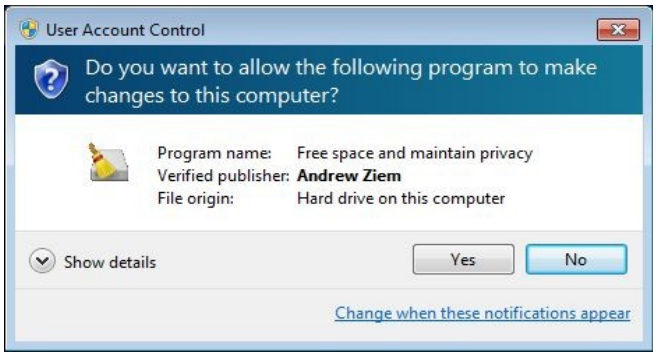
Последнее окно с вопросом, хотите ли вы запустить BleachBit прямо сейчас. Снимите выделение с пункта *Run BleachBit* и нажмите кнопку *Finish*.



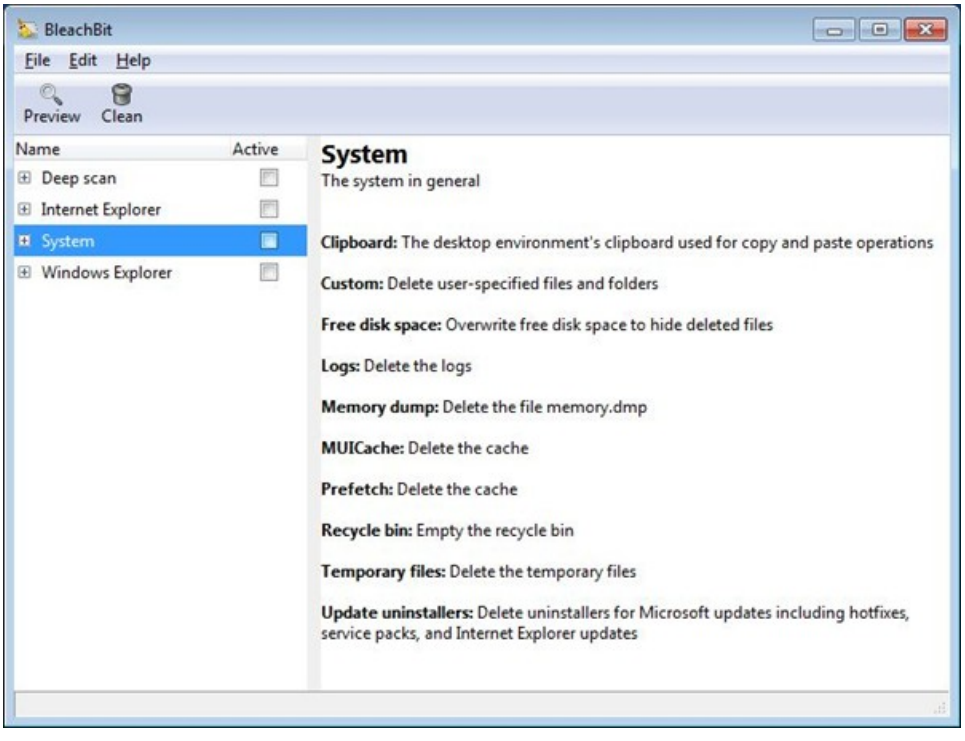
Использование BleachBit

Запустите BleachBit из меню «Пуск».

В небольшом окне появится вопрос, действительно ли вы хотите запустить BleachBit.

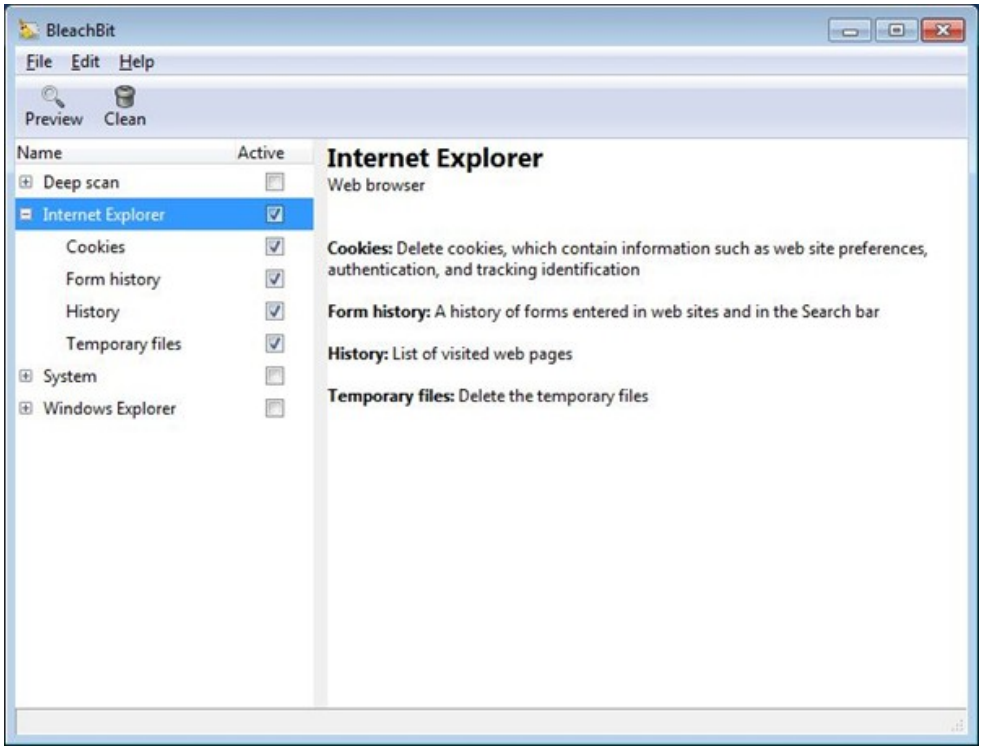


Главное окно. BleachBit определит несколько установленных популярных программ и покажет опции для каждой. По умолчанию в BleachBit четыре опции.

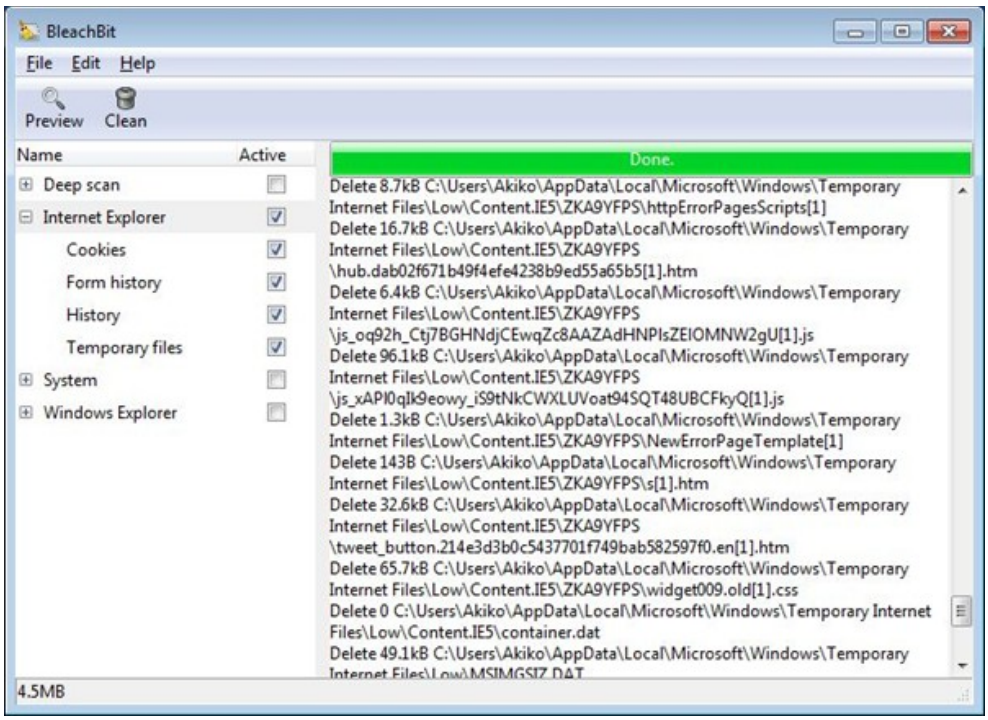


Использование шаблонов

BleachBit может избавляться от следов, которые оставляет браузер Internet Explorer, с использованием шаблона для IE (следы прочих браузеров BleachBit удалять не умеет). Отметьте поле *Internet Explorer*. Вы увидите, что автоматически окажутся выбраны поля *Cookies*, *Form history*, *History* и *Temporary files*. Можете снять выделение в каком-либо поле (или полях), если необходимо. Нажмите кнопку *Clean*.

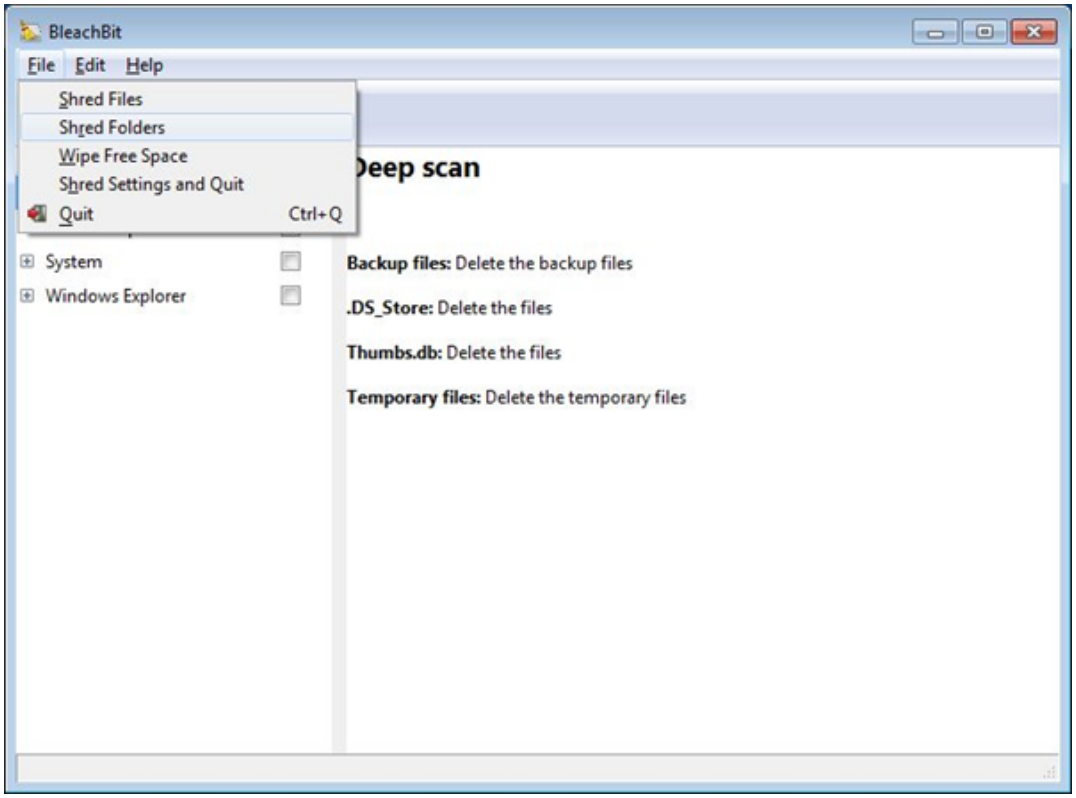


BleachBit выполнит удаление некоторых файлов. Вы увидите индикатор процесса.

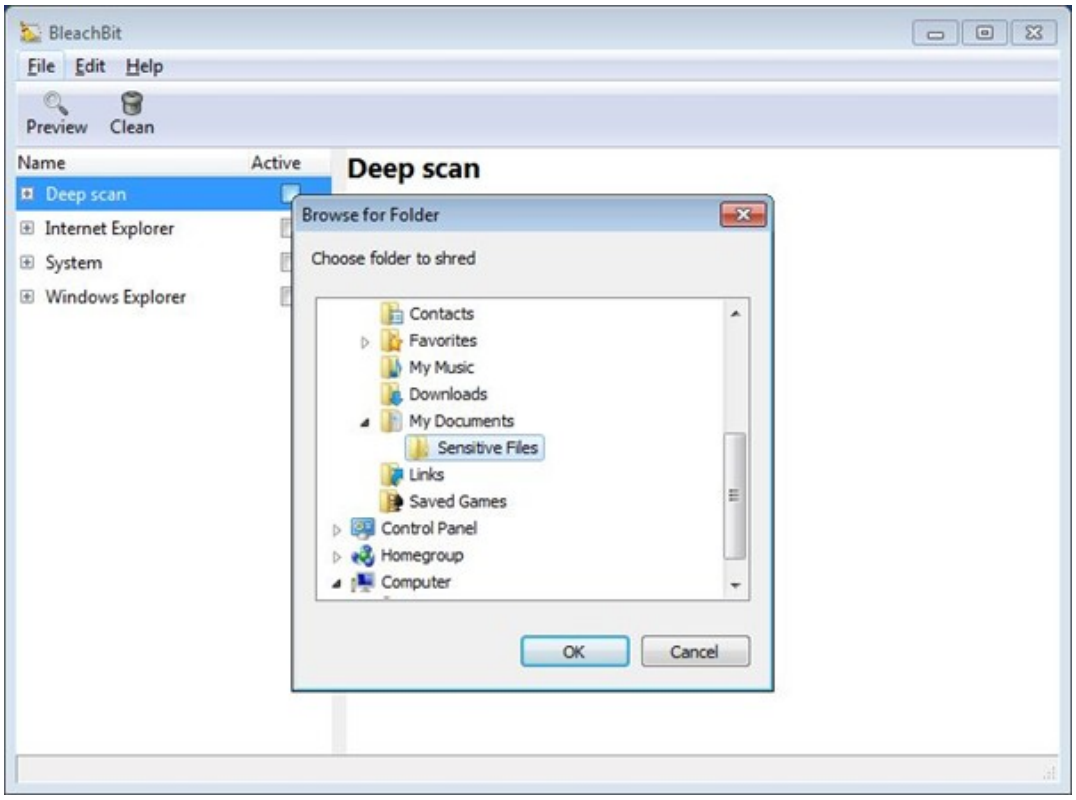


Надёжное удаление папки

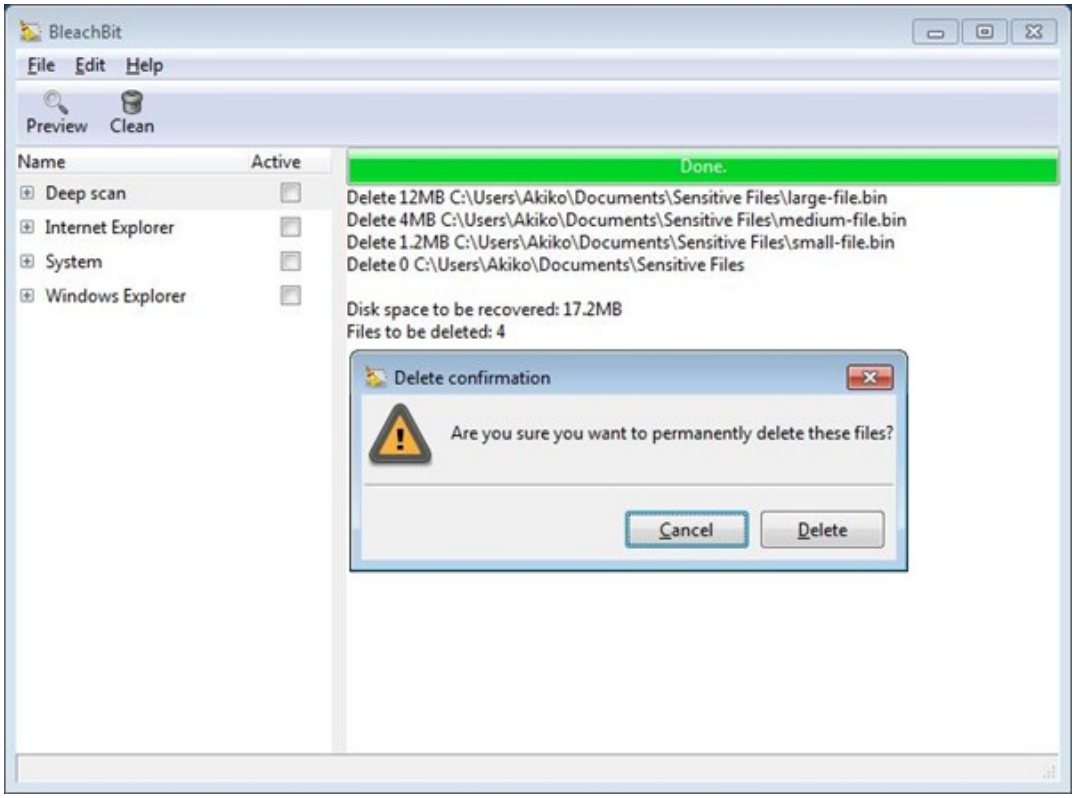
Выберите пункт меню *File* и далее *Shred Folders*.



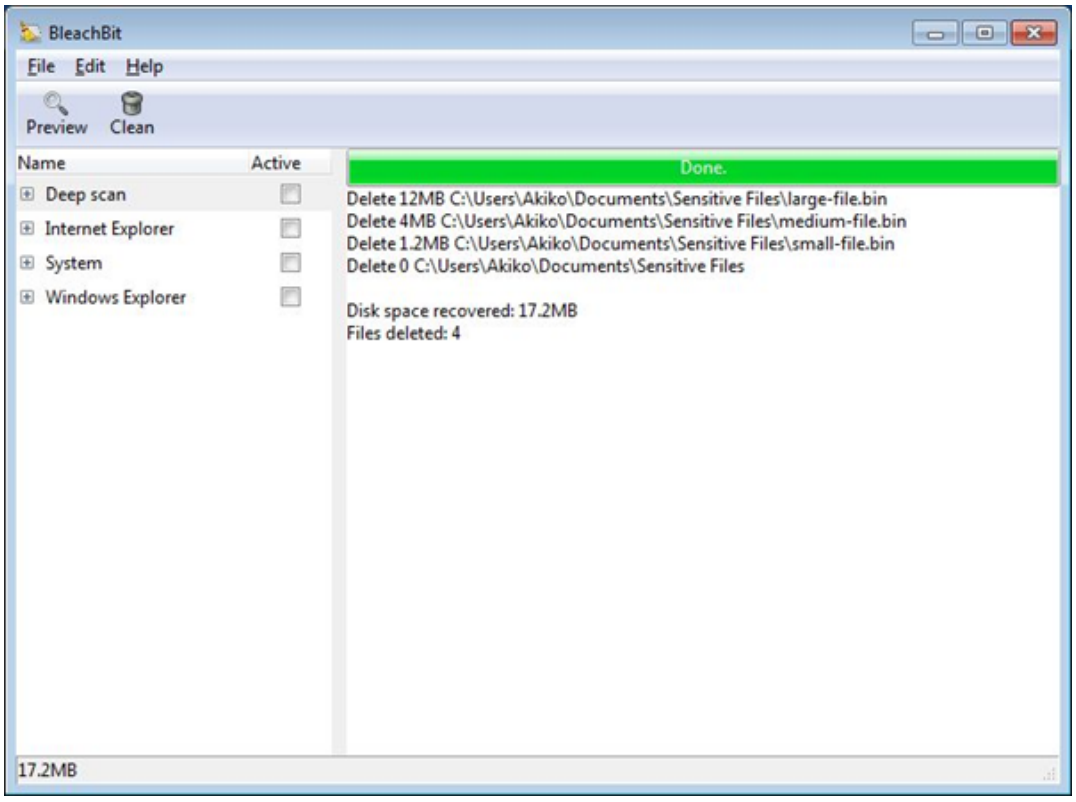
Появится маленькое окно. Выберите папку для удаления.



BleachBit попросит подтвердить, хотите ли вы навсегда удалить выбранные файлы. Нажмите кнопку *Delete*.

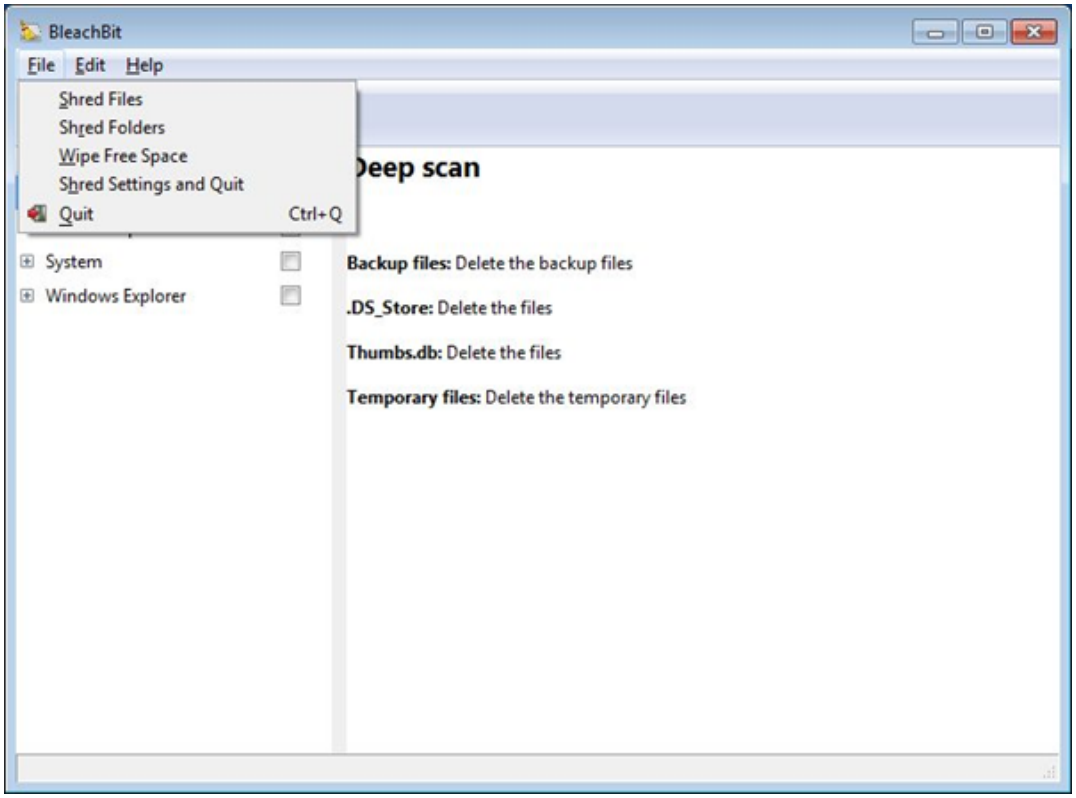


BleachBit покажет названия удалённых файлов. Обратите внимание, что BleachBit надёжно стирает каждый файл в папке, а затем собственно папку.

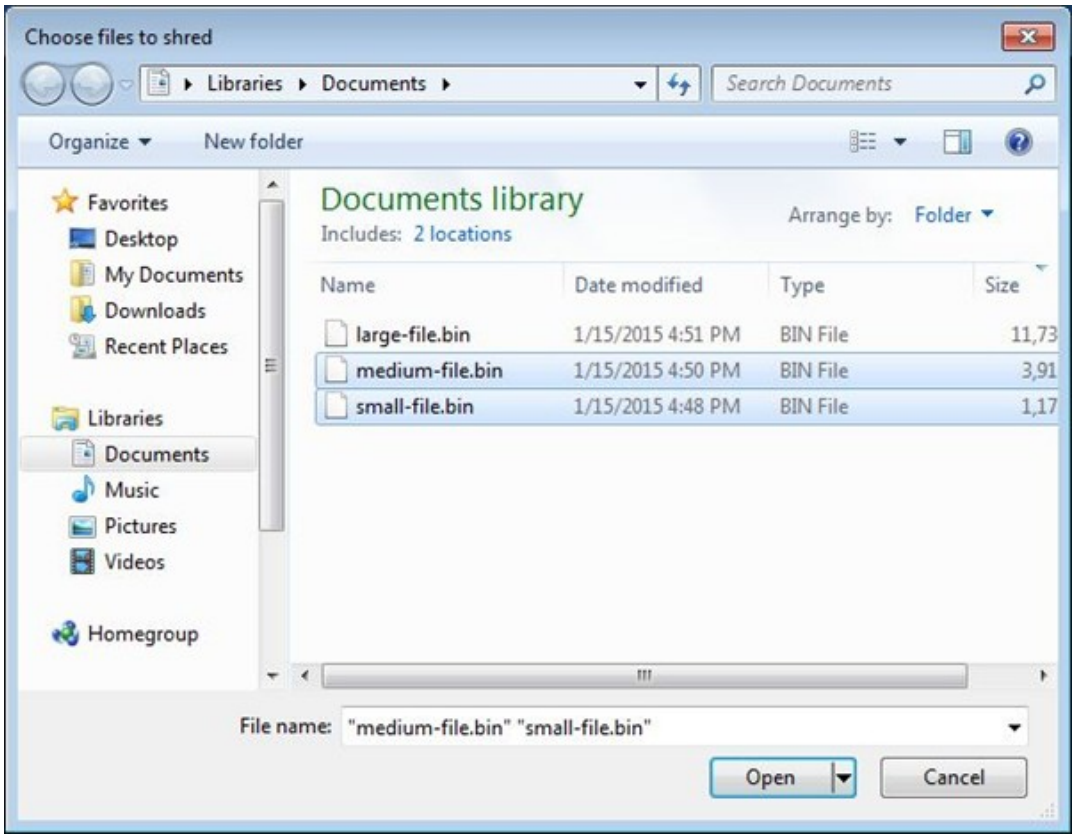


Надёжное удаление файла

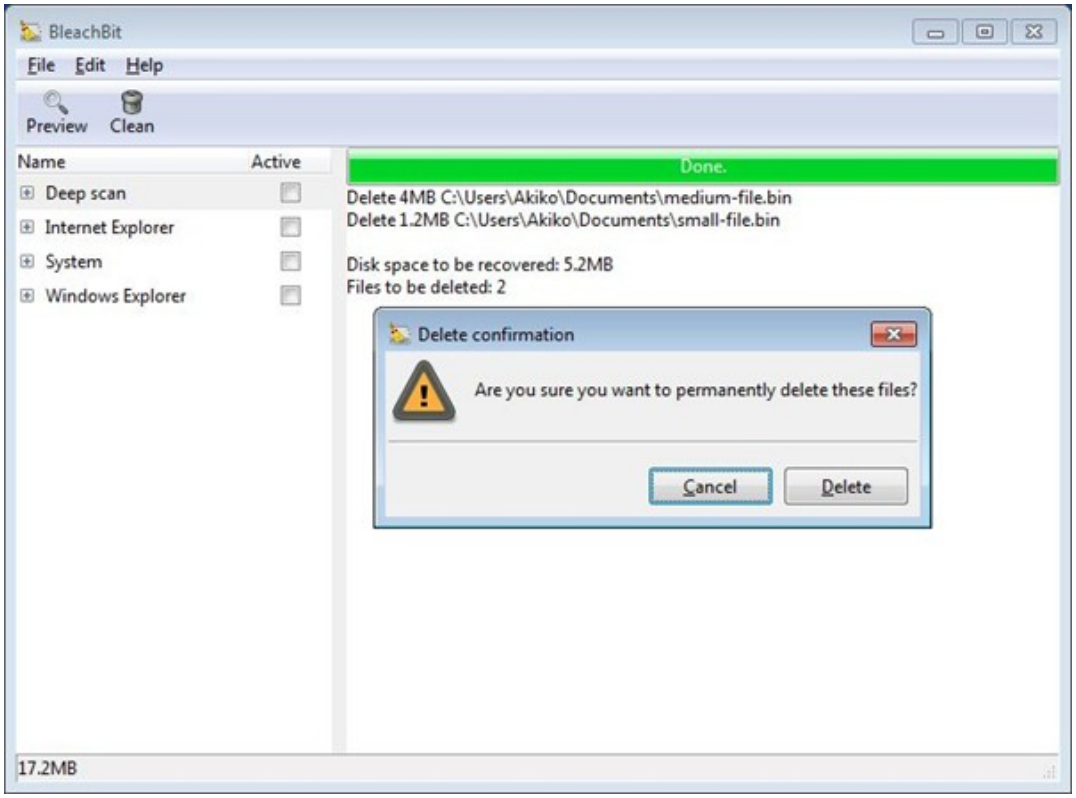
Выберите пункт меню *File* и далее *Shred Files*.



Откроется окно выбора файла. Выберите файлы для удаления.



BleachBit попросит подтвердить, хотите ли вы навсегда удалить выбранные файлы. Нажмите кнопку *Delete*.



У BleachBit есть много других функций. Самая полезная – «очистка свободного пространства». Таким образом можно избавиться сразу от всех следов когда-либо удалённых файлов. Windows часто оставляет фрагменты удалённых файлов и называет это пространство на жёстком диске свободным. Процедура очистки свободного пространства перезапишет всё это место случайными данными. Может понадобиться немало времени в зависимости от объёма жёсткого диска и свободного пространства.

Ограничения программ надёжного удаления данных

Первое: описанная процедура позволяет надёжно удалить только файлы на жёстком диске вашего компьютера. Она не затронет резервные копии, сохранённые на других дисках, USB-флешках, на сервере электронной почты, в облачном хранилище. Чтобы надёжно удалить файл со всеми его резервными копиями, нужно стереть **каждую из них, где бы они ни находились.** Кроме того, если файл сохранён в облачном хранилище (вроде Dropbox) или файлообменнике, обычно нет никаких гарантий, что его вообще удастся надёжно удалить.

Увы, это не единственная оговорка. Даже если вы последовали нашему совету и удалили все копии файла, существует вероятность, что некоторые следы файла остались на компьютере. Это происходит не из-за ошибки надёжного удаления файла, а благодаря операционной системе или другим программам, хранящим записи об этом файле.

Можно привести много примеров таких ситуаций. Мы ограничимся двумя. В операционных системах Windows или Mac OS, пакет Microsoft Office может хранить ссылку на файл в меню «Недавние документы», даже если сам файл уже удалён. Иногда Office может даже хранить копии актуального файла в специальном временном файле. В ОС Linux (и других операционных системах семейства *nix), OpenOffice может хранить не меньше записей о файлах, чем Microsoft Office, а в логах останутся команды, из которых можно узнать о названии файла, даже если сам файл был надёжно удалён. Программы, которые «ведут» себя подобным образом, встречаются на каждом шагу.

Что можно сделать в связи с этим? Вопрос непростой. Придётся признать, что даже после надёжного удаления файла его название может на какое-то время сохраниться в системе. Перезапись абсолютно всего диска – единственный способ на 100% убедиться, что имя файла больше нигде не осталось. Пытливый читатель спросит: «Что если кто-то изучит данные на диске байт за байтом? Можно ли определить наличие копий документа таким способом?» И да, и нет. Такая операция определит копии в текстовом формате, но если какое-то приложение использовало сжатие или иные способы обработки данных, это не получится. И помните: сам по себе поиск тоже может оставлять след! Таким образом, шанс найти копии файла существует,

хотя и невелик. Только полная перезапись всего диска и установка операционной системы заново могут дать гарантии, что файл или его фрагменты нигде не сохранились.

Хотите избавиться от диска? Не забудьте надёжно удалить данные!

Итак, диску пора на свалку, или вы собираетесь его подарить/продать. Важно знать, что никто не сможет извлечь из него вашу информацию. К сожалению, многие владельцы компьютеров забывают это делать. Жёсткие диски часто продаются, набитые важными данными. Перед тем, как расстаться с диском, надёжно удалите все данные. Ваш диск очень старый? Вы не верите, что им кто-нибудь заинтересуется? Осторожность всё равно не помешает. Есть программа специально для этой цели – **Darik's Boot and Nuke**.

В некоторых программах для шифрования диска встроена возможность уничтожения мастер-ключа. Это делает все зашифрованные данные недоступными навсегда. Поскольку ключ – крошечный объём данных, его можно уничтожить практически мгновенно. Такой подход позволяет сэкономить массу времени по сравнению с программами вроде Darik's Boot and Nuke (они могут работать очень долго на ёмких дисках). Но если вы не используете шифрование всего диска, придётся перезаписать все данные на носителе.

Уничтожение CD-ROM

Для компакт-дисков CD/DVD лучше использовать тот же подход, что и для бумажных носителей: шреддер. Существуют недорогие устройства, которые способны «переварить» ваши диски. Никогда не выбрасывайте CD в мусор, если не уверены на 100%, что на нём нет никакой важной информации.

Надёжное стирание данных на твердотельных накопителях (SSD), USB-флешках и SD-картах

К сожалению, технологически SSD-диски, USB-флешки и SD-карты делают трудным (если вообще возможным) надёжное стирание данных – как отдельных файлов, так и всего свободного пространства. Лучше всего выстраивать защиту данных на таких носителях на основе шифрования. Тогда информация, конечно, останется, но будет выглядеть как абракадабра для любого, кто получит её, не имея возможности заставить вас расшифровать данные. Сегодня мы не можем предложить какой-то конкретный работающий способ надёжного удаления данных с накопителя SSD.

Как было сказано ранее, SSD-диски и USB-флешки используют технологию под названием нивелирование износа. Вот как это работает. Пространство на диске разбивается на блоки подобно страницам книги. Когда происходит запись файла, ему сопоставляется конкретный блок или блоки (страницы). Если вы хотите перезаписать данные, вам следует сообщить, в каких блоках это нужно сделать. Но на носителях SSD и USB блоки «изнашиваются». Каждый блок может быть использован для записи и перезаписи ограниченное число раз, потом он теряет работоспособность (представьте, что вы пишете карандашом и стираете написанное ластиком; рано или поздно бумага придёт в негодность). Для решения этой проблемы контроллеры SSD-дисков и USB-флешек «заботятся» о том, чтобы число актов записи в каждый блок было примерно одинаковым по всему носителю. Это позволяет продлить ему жизнь. Бывает, что вместо перезаписи конкретного блока, где изначально находился файл, диск не трогает этот блок, помечает его как неработающий и записывает данные в другой блок (вы пропускаете страницу, записываете нужное на соседнюю и делаете исправления в содержании книги). Такие действия происходят на низком уровне, в электронике диска, и операционная система даже не знает об этом. Соответственно, если вы хотите перезаписать файл, нет гарантий, что это произойдёт. Это и есть главная причина, по которой так трудно надёжно удалить данные с накопителя SSD.