

# Руководство пользователя

---



## DriveCleanser 6.0

---

Copyright © SWsoft, 2000–2002 All rights reserved.

OS/2 — зарегистрированный товарный знак IBM Corporation.

Windows — зарегистрированный товарный знак Microsoft Corporation.

Все остальные упоминаемые товарные знаки могут быть зарегистрированными товарными знаками тех или иных фирм.

Распространение настоящих и/или переработанных материалов, входящих в данное руководство, в виде печатного издания (книги) запрещено без письменного разрешения их владельца.

ДОКУМЕНТАЦИЯ ПОСТАВЛЯЕТСЯ «КАК ЕСТЬ». НЕ СУЩЕСТВУЕТ НИКАКИХ ЯВНО ВЫРАЖЕННЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ОБЯЗАТЕЛЬСТВ, ПОДТВЕРЖДЕНИЙ ИЛИ ГАРАНТИЙ, В ТОМ ЧИСЛЕ И СВЯЗАННЫХ С ТОВАРНОСТЬЮ ПО, ПРИГОДНОСТЬЮ В ОПРЕДЕЛЕННЫХ ЦЕЛЯХ, НАСКОЛЬКО ТАКАЯ ОГРАНИЧЕННОСТЬ ОТВЕТСТВЕННОСТИ ДОПУСКАЕТСЯ ЗАКОНОМ.

# Содержание

<b>ГЛАВА 1. ВВЕДЕНИЕ.....</b>	<b>4</b>
<b>ГЛАВА 2. УСТАНОВКА И НАЧАЛО РАБОТЫ С ACRONIS DRIVECLEANSER.....</b>	<b>9</b>
2.1 КОМПЛЕКТ ПОСТАВКИ .....	9
2.2 УСТАНОВКА ПРОГРАММЫ .....	9
2.3 ОБНОВЛЕНИЕ ACRONIS DRIVECLEANSER.....	10
2.4 УДАЛЕНИЕ СИСТЕМЫ .....	10
2.5 ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС .....	10
<b>ГЛАВА 3. РАБОТА С ПРОГРАММОЙ ACRONIS DRIVECLEANSER .....</b>	<b>12</b>
3.1 ИСПОЛЬЗОВАНИЕ ПРЕДУСТАНОВЛЕННЫХ АЛГОРИТМОВ .....	
УНИЧТОЖЕНИЯ .....	14
3.2 СОЗДАНИЕ ПОЛЬЗОВАТЕЛЬСКИХ АЛГОРИТМОВ УНИЧТОЖЕНИЯ .....	
ИНФОРМАЦИИ .....	17
<b>ПРИЛОЖЕНИЕ А. АЛГОРИТМЫ УНИЧТОЖЕНИЯ ДАННЫХ.....</b>	<b>28</b>

# Глава 1. Введение

## Что такое Acronis DriveCleanser

Acronis DriveCleanser гарантированно уничтожает все данные на выбранных разделах или/и дисках компьютера, предоставляя возможность использовать — в зависимости от степени важности информации — один из существующих стандартов уничтожения данных и создавать собственные алгоритмы.

## Конфиденциальная информация на жестких дисках: хранение и доступ

В настоящее время все большее количество информации создается в цифровой форме или переводится в нее и доверяется для хранения компьютерам. На жестких дисках хранятся документы, ранее создававшиеся исключительно с помощью печатной машинки, таблицы, файлы баз данных, мультимедийные файлы.

На жестких дисках хранится колоссальное количество персональных данных, в том числе таких важных и не предназначенных для посторонних глаз, как номера банковских лицевых счетов и кредитных карточек, данных деловых приложений — банковских, финансовых, бухгалтерских, производственного назначения. Перечислить все существующие документы и данные, которые ни в коем случае не должны попасть в руки лиц с криминальными наклонностями или просто конкурентов, не представляется возможным — настолько велико их многообразие.

Основное свойство этих документов, с точки зрения данного Руководства, заключается в том, что они содержат **конфиденциальную информацию**.

## Конфиденциальная информация: уничтожение

Однако иногда упускается из вида, что для обеспечения конфиденциальности информация должна не только **храниться** по специально разработанным правилам, но и **уничтожаться** по строгим правилам.

В самом деле, компьютеры на протяжении срока службы, как правило, неоднократно модернизируются. При этом, в связи с непрерывным ростом хранящихся на дисках объемов данных, часто в первую очередь модернизируется именно дисковая подсистема компьютера. На компьютер устанавливается диск большей емкости, данные со старого диска переносятся на новый, но при этом зачастую забывается то обстоятельство, что данные остаются и на старом диске.

Неосторожное хранение ненужного более жесткого диска легко может привести к утрате конфиденциальной информации. Лучше всего сразу после того, как данные будут перенесены на новый диск, полностью **уничто-**

**жить** их на старом диске. Уничтожить! Не стереть информацию, не удалить более ненужные файлы, а именно уничтожить! (Различие между удалением файлов и уничтожением информации будет разьяснено далее.)

Можно привести следующую яркую иллюстрацию сказанному выше:

«Американец Джек Вильсон, компьютерный консультант из Брайтона, приобрел ноутбук IBM ThinkPad 600E за 400 долларов на распродаже имущества обанкротившихся интернет-компаний. Выяснилось, что на жестком диске содержатся данные о софтверной компании IPHighway, которая к тому моменту уже не работала. Среди этих данных были номера карт социального обеспечения и величина заработной платы 46 сотрудников фирмы, платежные ведомости, стратегические планы компании, закрытые решения совета директоров и другие внутренние документы.

Это не единичный случай приобретения конфиденциальной информации при покупке бывшего в употреблении компьютера».

(Источник: [www.zdnet.com](http://www.zdnet.com), 20 Августа, 2001, со ссылкой на Wall Street Journal Online.)

### **Удаление данных средствами операционных систем**

Между удалением файлов с данными средствами операционной системы (с помощью файловых менеджеров) и уничтожением информации специализированными программами есть существенное различие.

Дело в том, что, например, такая операционная система, как Windows, при **удалении файла** реально ничего с жесткого диска не удаляет: просто имя удаляемого файла в Таблице размещения файлов (File Allocation Table, FAT) заменяется на имя, которое операционная система не считает корректным. Поэтому файл становится невидимым для пользователя, цепочка кластеров, содержащих данные файла, считается далее свободной. Но информация, содержащаяся в секторах жесткого диска, остается неизменной. Для специалиста восстановить ее не составит труда. Существуют многочисленные программы, выполняющие эту функцию в DOS и Windows.

Несколько более надежным является удаление файлов в операционной системе Linux, но и здесь для восстановления действительно важной информации можно привлечь необходимые средства, в том числе программные.

Не решает проблему ни **удаление разделов** на диске, ни даже **форматирование** жесткого диска. При удалении разделов на жестком диске стирается информация Таблицы разделов (Partition table, если это первичный раздел) и Таблицы размещения файлов. Информация же, размещенная в секторах остается нетронутой и может быть восстановлена специальными средствами.

Надежное уничтожение информации на жестких дисках возможно только с использованием специально разработанных программ, реализующих специально разработанные алгоритмы.

### **Гарантированное уничтожение конфиденциальной информации: стандарты**

Под гарантированным уничтожением информации на магнитных носителях понимается невозможность ее восстановления квалифицированными специалистами с помощью любых известных устройств и способов реставрации.

Гарантированное уничтожение конфиденциальной информации на жестких магнитных дисках с помощью специальных алгоритмов предлагает программа Acronis DriveCleanser.

Acronis DriveCleanser реализует строгие алгоритмы гарантированного уничтожения конфиденциальной информации, удовлетворяющие наиболее известным национальным стандартам:

- (1) американскому: U.S. Standard, DoD 5220.22-M;
- (2) американскому: NAVSO P-5239-26 (RLL);
- (3) американскому: NAVSO P-5239-26 (MFM);
- (4) немецкому: VSITR;
- (5) российскому: Russian Standard, GOST P50739-95.

Помимо алгоритмов, соответствующих национальным стандартам, Acronis DriveCleanser поддерживает predetermined алгоритмы, предложенные известными и авторитетными специалистами в области защиты информации:

- (6) алгоритм Питера Гутмана — данные на жестком диске уничтожаются за 35 проходов,
- (7) алгоритм Брюса Шнайера — данные уничтожаются за 7 проходов.

Кроме того, программа Acronis DriveCleanser поддерживает простой, но быстрый алгоритм уничтожения информации, предусматривающий единственный проход по жесткому диску с обнулением всех секторов.

Важнейшей особенностью программы Acronis DriveCleanser является возможность создания пользователем своих **собственных алгоритмов** уничтожения данных.

Детальное описание теории и алгоритмов уничтожения данных, поддерживаемых Acronis DriveCleanser, дано в Приложении А. «Алгоритмы уничтожения данных» к данному Руководству.

## **Как найти нужный вам раздел Руководства**

Программа Acronis DriveCleanser проста и интуитивно понятна как с точки зрения пользовательского интерфейса, так и с точки зрения последовательности работы с ней. Тем не менее, чтобы заинтересованному пользователю было легче ориентироваться в содержании руководства, отметим следующее:

1. более подробную информацию о том, почему столько внимания уделяется специальным алгоритмам уничтожения информации на жестких дисках, можно найти в Приложении А. «Алгоритмы уничтожения данных »;
2. об уничтожении данных при помощи Acronis DriveCleanser рассказывается в Главе 2 в разделе 3.1 «Использование предустановленных алгоритмов уничтожения».
3. создание собственных алгоритмов уничтожения данных изложено в Главе 2 в разделе 3.2 «Создание пользовательских алгоритмов уничтожения информации».

## **Условия использования системы**

Условия использования системы Acronis DriveCleanser изложены в «Лицензионном соглашении», которое входит в поставку системы. Подтверждением того, что система Acronis DriveCleanser приобретена и используется вами легально, служит входящая в поставку регистрационная карточка. Каждая регистрационная карточка имеет индивидуальный регистрационный номер.

С точки зрения действующего законодательства «Лицензионное соглашение» рассматривается как договор между пользователем и производителем программного обеспечения. Договор имеет юридическую силу, и его нарушение может повлечь за собой судебное разбирательство.

Нелегальное использование и распространение программного обеспечения преследуется по закону.

## **Служба технической поддержки**

Пользователям легально приобретенных и зарегистрированных копий Acronis DriveCleanser предоставляется бесплатная техническая поддержка со стороны компании Acronis . В том случае, если у вас возникли проблемы при установке или эксплуатации системы, и вы не смогли решить их, руководствуясь данной документацией, обратитесь в службу технической поддержки по электронной почте.

Перед обращением вам необходимо зарегистрировать программу через Интернет по адресу <http://www.acronis.ru/registration/> либо по обычной почте.

При обращении в службу технической поддержки необходимо назвать регистрационный номер используемой вами копии Acronis DriveCleanser. Регистрационный номер указан на регистрационной карточке, входящей в поставку системы.

WWW: <http://www.acronis.ru/support/>

E-mail: [support@acronis.ru](mailto:support@acronis.ru)



# Глава 2. Установка и начало работы с Acronis DriveCleanser

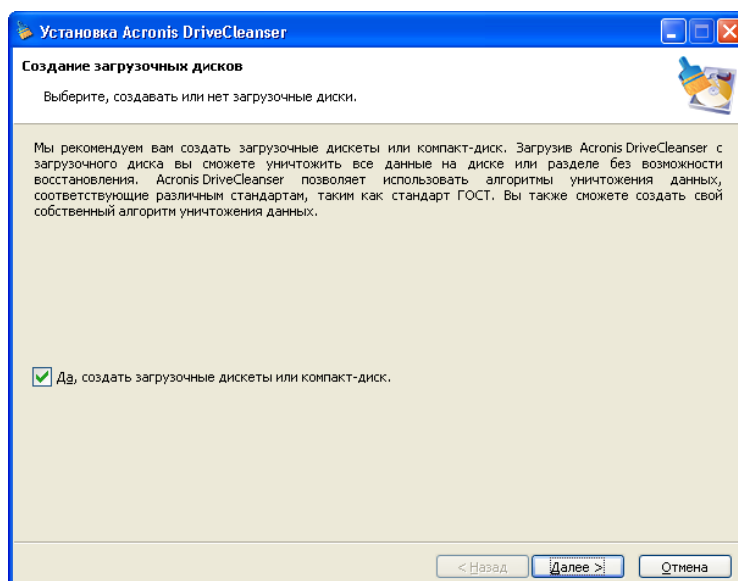
## 2.1 Комплект поставки

- В поставку системы Acronis DriveCleanser входит следующее:
- один установочный диск,
- данная документация,
- лицензионное соглашение,
- регистрационная карточка,
- рекламно-информационные материалы.

## 2.2 Установка программы

Для установки Acronis DriveCleanser:

1. Вставьте CD-ROM в устройство чтения компакт-дисков и запустите программу установки.
2. Тщательно следуйте всем указаниям программы.
3. После ответов на вопросы программы и копирования файлов DriveCleanser на жесткий диск вам будет предложено создать загрузочный CD или дискету. Обычно, DriveCleanser работает непосредственно в операционной системе (ОС) Windows, однако, вам может быть необходимо перенести данные с жесткого диска с ОС Linux или любой другой. В этом случае рекомендуется создать загрузочный диск и загрузить при помощи него ваш компьютер.



После установки вам необходимо перезагрузить компьютер.

## 2.3 Обновление Acronis DriveCleanser

Для обновления и/или восстановления Acronis DriveCleanser запустите программу установки Acronis DriveCleanser еще раз. Программа установки определит, что Acronis DriveCleanser уже устанавливался на ваш компьютер и спросит вас о том, хотите ли вы восстановить (обновить) программу или полностью удалить ее с диска.

## 2.4 Удаление системы

Для удаления программы в меню Programs выберите **Acronis → DriveCleanser → Удалить Acronis DriveCleanser**. На экране появится окно диалога с запросом о подтверждении удаления программы с жесткого диска вашего компьютера. Для подтверждения удаления нажмите кнопку **Да**. Программа Acronis DriveCleanser будет полностью удалена.

## 2.5 Пользовательский интерфейс

Программа Acronis DriveCleanser имеет Windows-подобный графический интерфейс пользователя и управляется с помощью мыши или клавишами **Tab**, **Shift+Tab**, **←**, **→**, **↑**, **↓**, **Space**, **Enter** и **Escape**.



Если вы регулярно работаете с приложениями под Windows, X Window или OS/2, то проблем с пониманием и использованием интерфейса Acronis DriveCleanser у вас не возникнет.

В процессе работы с программой Acronis DriveCleanser пользователь имеет дело с последовательностью **окон диалога**, в каждом из которых ему предлагается осуществить выбор одного из нескольких возможных в дальнейшем действий, установив переключатель определенного вида в нужное положение или выбрав одно из значений из списка, или отметив для работы нужные разделы или диски. Такой вариант интерфейса также называется **мастером**.

Нужное положение (состояние) переключателя **выбирается** (устанавливается) с помощью мыши или нажатием клавиш.

В каждом окне диалога представлен подробный текстовый комментарий к назначению окна и представленного на нем списка (или переключателя), а также к каждому элементу списка (возможному состоянию переключателя).

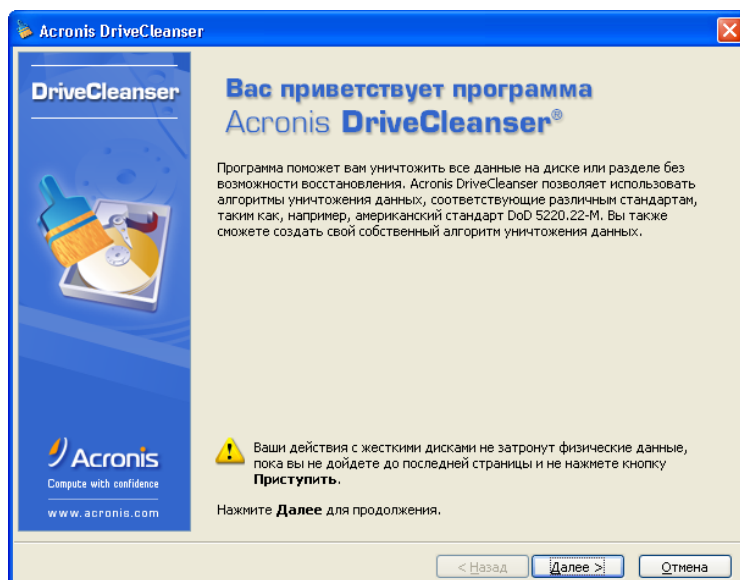


В окнах мастера отсутствует специальная кнопка **Справка**. В данном случае в ней нет необходимости, так как в каждом окне подробно рассказывается о назначении окна и находящихся в нем элементов управления. Более того, подробно рассказывается, какие возможности предоставит программа, если вы установите конкретный переключатель в любое из доступных состояний.

## Глава 3. Работа с программой Acronis DriveCleanser

Работа с программой Acronis DriveCleanser начинается с экрана приглашения. Экран сообщает вам об основных возможностях программы; к ним относятся:

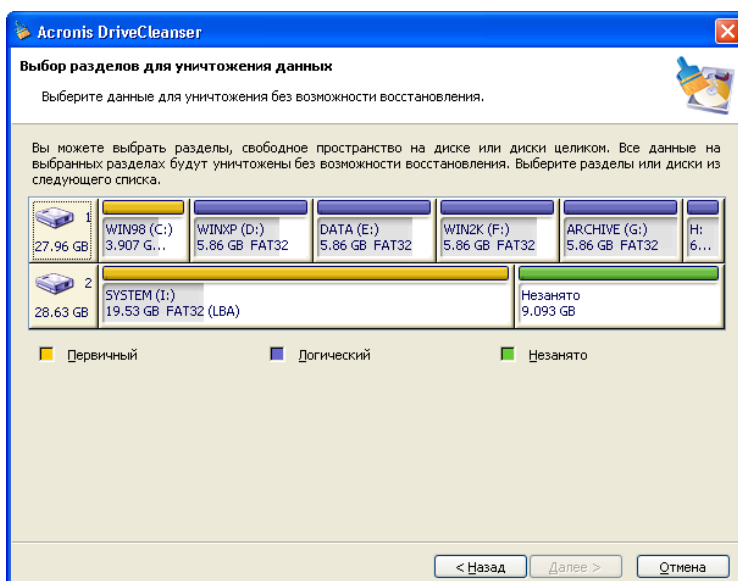
1. очистка выбранных разделов жесткого диска (дисков) от содержащейся в них информации с помощью одного из предустановленных алгоритмов;
2. создание и использование пользовательских алгоритмов очистки жесткого диска.



### Окно приглашения к работе программы Acronis DriveCleanser

Все действия над жесткими дисками осуществляются на основе создаваемых в процессе диалога с пользователем **сценариев**. До того, как вы запустите созданный сценарий на выполнение, никаких реальных действий по уничтожению информации не происходит. На любом этапе работы с программой вы можете вернуться к предыдущим этапам создания сценария и выбрать для уничтожения другие разделы и/или диски или другие алгоритмы очистки жесткого диска.

В следующем окне вам будет представлен список жестких дисков, подключенных к вашему компьютеру, и разделов на них с их основными параметрами (емкостью дисков и размерами разделов, файловыми системами и метками).



### Список жестких дисков компьютера (с разделами)

Для дальнейшей работы вы должны выбрать разделы жестких дисков, на которых вы хотите уничтожить информацию.

Щелкните мышью на прямоугольнике, представляющем раздел жесткого диска. В правом верхнем углу прямоугольника появится красный крест. Это означает, что раздел выбран для уничтожения содержащейся на нем информации.

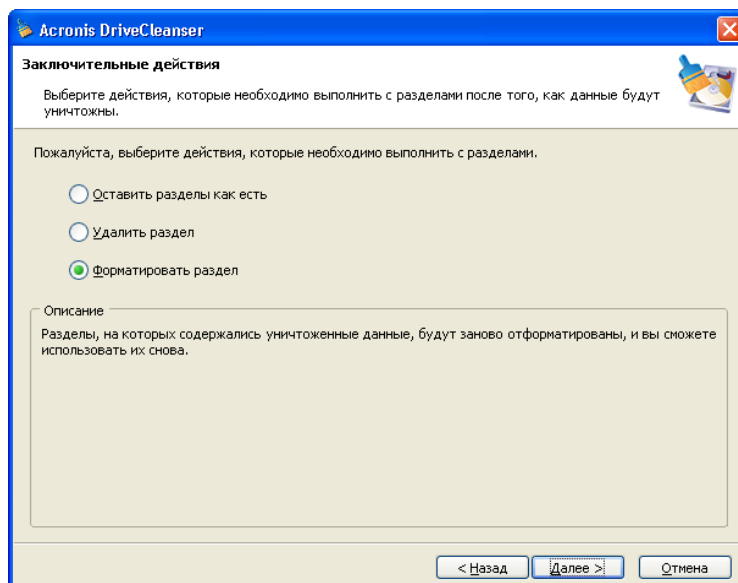
Вы можете выбрать для уничтожения информации диск целиком (или несколько дисков). Для этого щелкните мышью на прямоугольнике, представляющем жесткий диск (со значком устройства, номером диска и его емкостью).

Вы можете одновременно выбрать несколько различных разделов, расположенных на разных дисках, или несколько дисков.

Для продолжения работы щелкните мышью на кнопке **Далее**.

В окне **Заключительные действия** вы можете выбрать, что делать с разделом, информация на котором уничтожается. Acronis DriveCleanser предоставляет вам три возможности:

- **Оставить раздел как есть** — то есть только уничтожить информацию в соответствии с алгоритмом, который вам будет предложено выбрать ниже;
- **Удалить раздел** — уничтожить информацию и удалить раздел;
- **Форматировать раздел** — уничтожить информацию и отформатировать раздел (установлено по умолчанию).

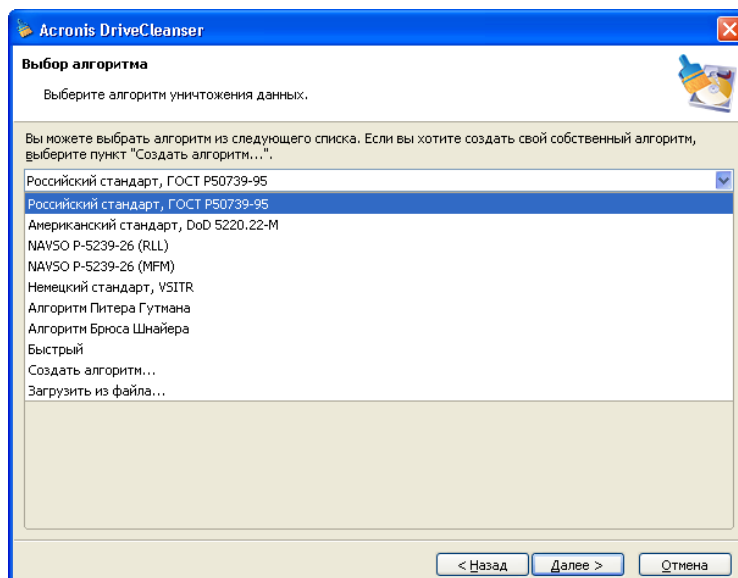


### Окно Заклучительные действия

В приведенном ниже примере предполагается, что переключатель установлен в положение **Оставить разделы как есть**. Это позволит увидеть, к каким результатам приводит уничтожение информации раздела само по себе (без форматирования или удаления раздела).

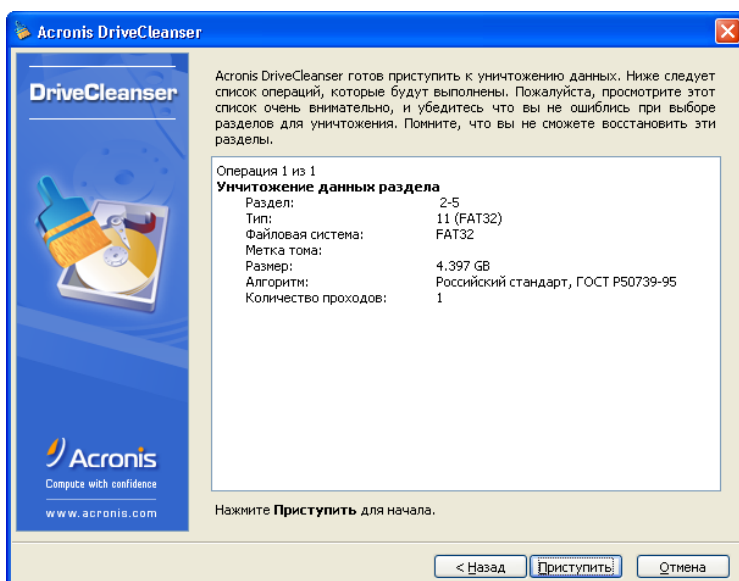
## 3.1 Использование предустановленных алгоритмов уничтожения

В следующем окне **Выбор алгоритма** вы должны выбрать из списка один из предустановленных алгоритмов очистки жесткого диска.



### Предопределенные алгоритмы в списке

Следующее окно представляет созданный сценарий очистки разделов жесткого диска.



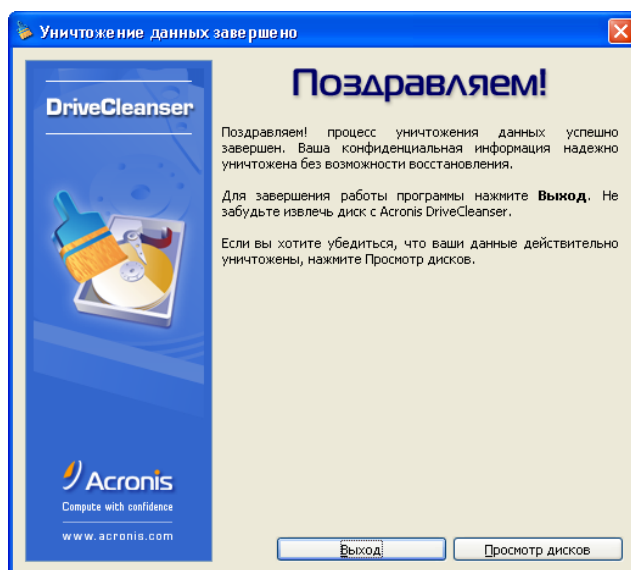
#### Окно сценария очистки жесткого диска

В данный момент программа Acronis DriveCleanser готова к выполнению процедуры очистки.

Для запуска сценария очистки разделов жесткого диска на выполнение щелкните мышью на кнопке Приступить.

После нажатия кнопки Приступить Acronis DriveCleanser продолжит процесс очистки жесткого диска автоматически. В большинстве случаев для этого потребуется перезагрузка вашего компьютера.

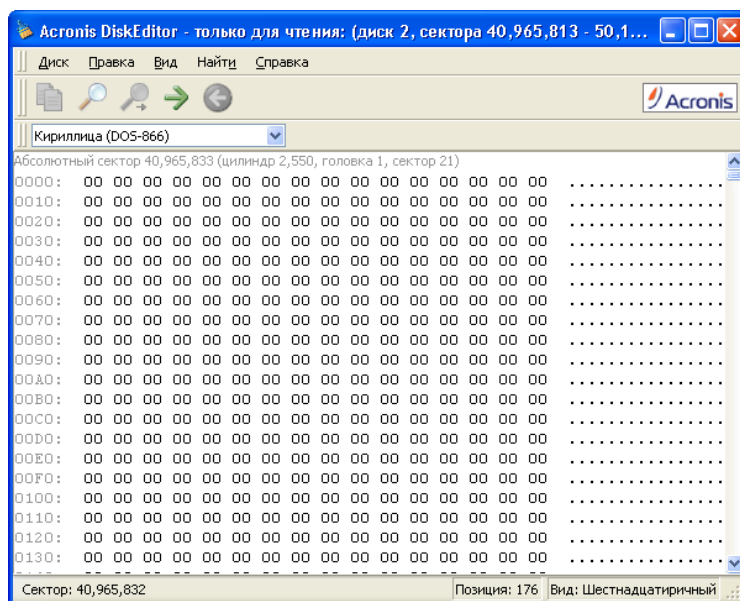
По завершении очистки жесткого диска вы получите сообщение об успешном завершении процедуры очистки диска.



### Окно сообщения об успешном завершении процедуры очистки

Программа Acronis DriveCleanser предоставляет вам еще одну возможность — оценить результаты выполнения процедуры (алгоритма) очистки раздела или/и жесткого диска. Acronis DriveCleanser имеет встроенную программу просмотра жесткого диска DiskViewer.

Рассмотренные выше алгоритмы предлагают различные варианты уничтожения конфиденциальной информации. Таким образом, картина, которую вы увидите на разделе или/и диске зависит от выбранного до этого алгоритма уничтожения информации, но фактически вы можете увидеть сектора, заполненные либо нулями, либо случайными символами.



### Сектор раздела диска после применения быстрого алгоритма

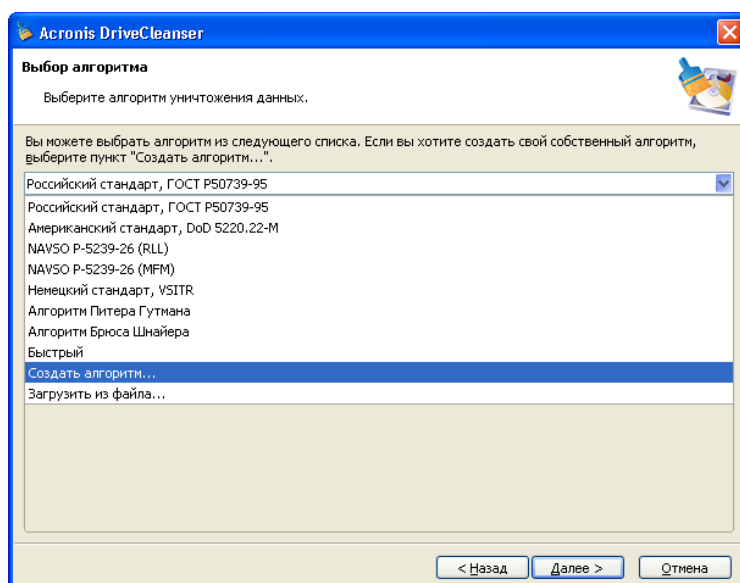


## 3.2 Создание пользовательских алгоритмов уничтожения информации

Программа Acronis DriveCleanser предоставляет пользователю возможность использовать для очистки жестких дисков не только предустановленные алгоритмы, но и создать свои собственные. Несмотря на то, что в программу включены алгоритмы всех классов — быстрые, но не слишком надежные, очень надежные, но медленные, компромиссные между теми и другими, — квалифицированный пользователь может почувствовать необходимость в своих собственных алгоритмах.

### Создание пользовательского алгоритма

Итак, для создания собственного алгоритма очистки жесткого диска в окне **Выбор алгоритма** в списке предустановленных алгоритмов найдите строку «Пользовательский алгоритм...» и щелкните по ней мышью. Обратите внимание, что в списке также присутствует строка «Загрузить из файла...».

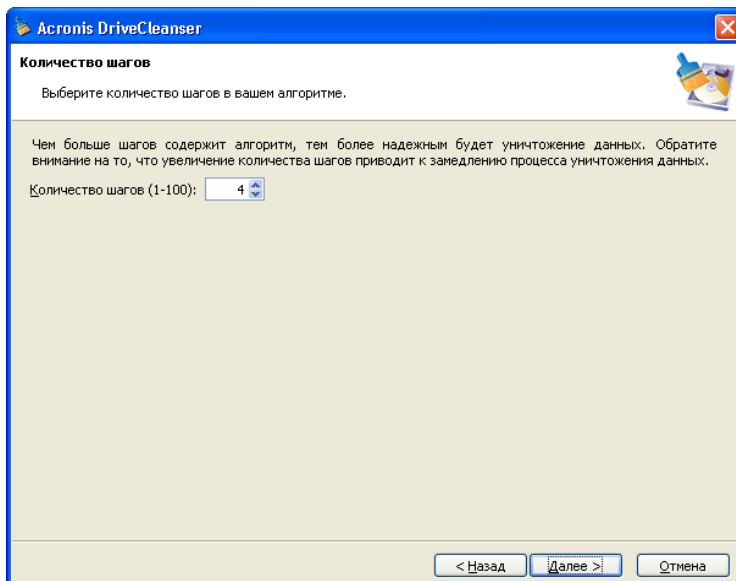


### Выбор создания пользовательского алгоритма

После выбора одного из предустановленных алгоритмов на экране сразу появлялось окно сценария очистки раздела жесткого диска (раздел и/или жесткий диск выбирался на одном из предыдущих шагов). На этот раз будет запущен мастер создания пользовательского алгоритма, в результате чего вы попадете в окно **Количество шагов**.

Давайте создадим в качестве иллюстрации простой пользовательский алгоритм, аналогичный, например, американскому стандарту. Как вы, вероятно, помните, американский стандарт предполагает три прохода по жесткому диску, во время которых на диск пишутся разного рода

символы, плюс еще один проход, во время которого осуществляется процедура верификации, — итого 4 прохода.



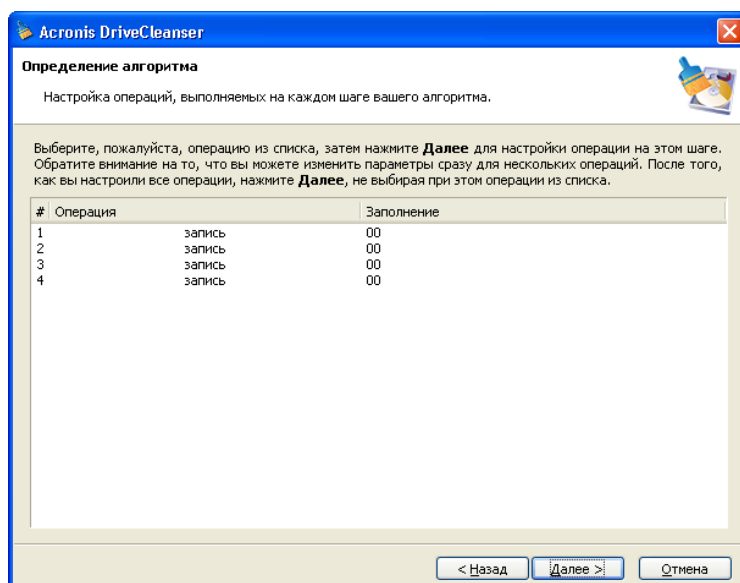
#### Окно Количество шагов пользовательского алгоритма

Напомним, что предустановленные алгоритмы для очистки жесткого диска выполняют от 1 (быстрый алгоритм, российский стандарт) до 35 проходов (алгоритм Питера Гутмана).

Вы можете ввести в поле (спинер), представленное в окне мастера, любое значение с клавиатуры или установить его с помощью мыши. В нашем примере введите в это поле значение равное 4.

## Определение алгоритма: шаблон

В окне **Определение алгоритма** вам представляется нечто вроде шаблона будущего алгоритма: список в этом окне содержит столько записей, сколько проходов вы определили для своего алгоритма на предыдущем этапе. (Шаблон этот, как вы легко можете видеть, вполне осмыслен, даже если вы ничего в нем не будете менять, он будет работать, затирая данные на жестком диске.)



### Окно определения алгоритма

Обозначения в окне имеют следующее значение. В первой колонке списка находится номер прохода по диску; во второй — тип операции над диском (таких операции всего две: запись на диск символа, «запись», и верификация, «проверка», записанного); в третьей колонке содержится записываемый на диск образец.

Записываемый на диск образец — это всегда шестнадцатеричное число, то есть число, например, вида: 0x00, 0xAA или 0xCD и т.п. В данном случае приведены числа длиной 1 байт, но они могут иметь длину до 512 байт. Кроме таких чисел вы можете ввести для записи случайное шестнадцатеричное число любой длины (до 512 байт; 512 байт — это, как вы помните, длина области данных сектора). Наконец, вы можете включить в алгоритм для записи еще одно число, обозначаемое как «дополнительный код числа», то есть число, дополнительное к записанному на диск на предыдущем проходе.

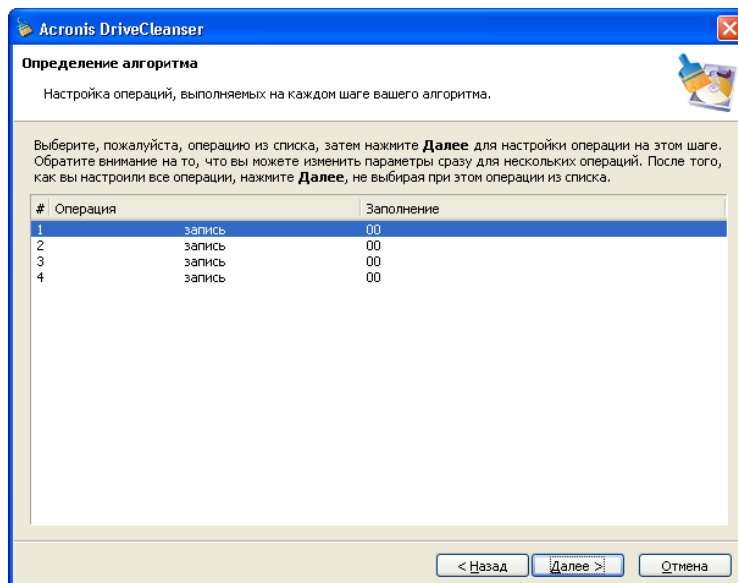
Таким образом вы можете включить в алгоритм следующие числа:

- произвольные шестнадцатеричные числа длиной 1–512 bytes;
- случайные шестнадцатеричные числа длиной (1–512 bytes);

- шестнадцатеричные числа, дополнительные к записанным на предыдущем проходе жесткого диска.

В окне **Определение алгоритма** вам предложен только шаблон алгоритма. Что именно программа должна писать на диск, чтобы уничтожить конфиденциальную информацию в соответствии с создаваемым вами алгоритмом, вы должны определить сами.

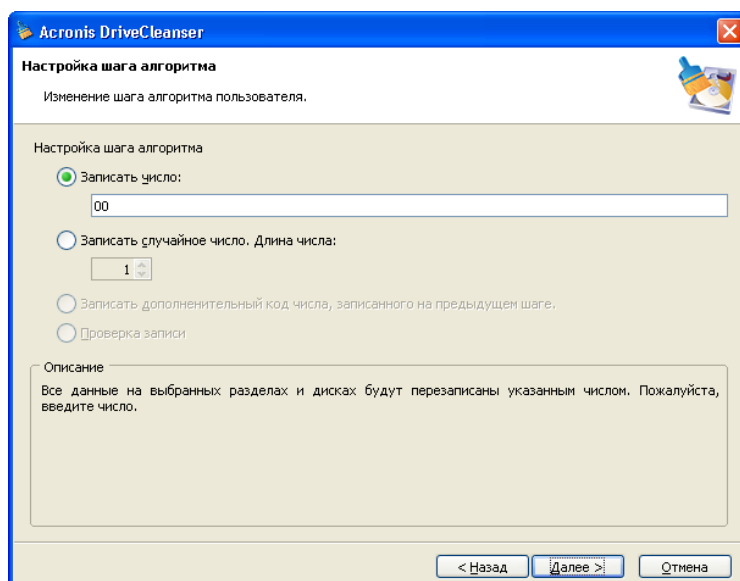
Для этого щелкните мышью, например, на строке, представляющей проход № 1.



### Выбор 1-го шага для определения образца

Для продолжения работы нажмите кнопку **Далее**.

На экране появится окно, в котором вы сможете определить записываемый на диск образец (шестнадцатеричное число).



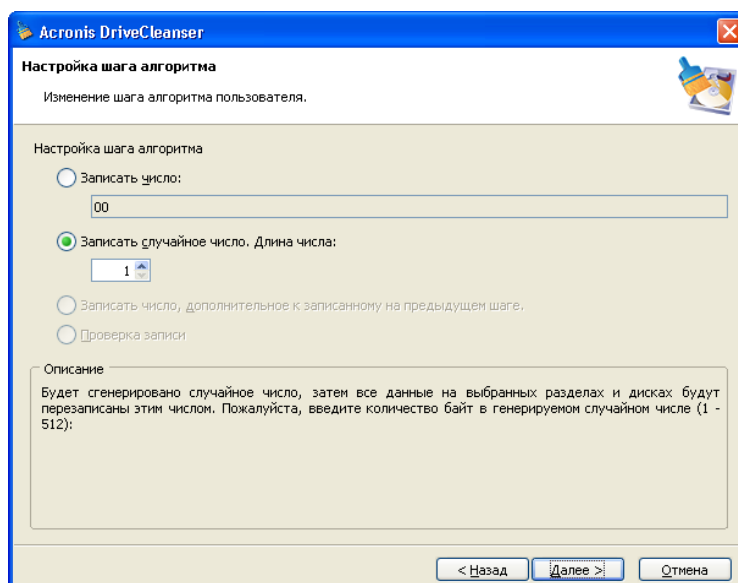
### Окно определения записываемых образцов

На этом рисунке, по умолчанию, переключатель установлен в положение **Записать число**, в поле введено шестнадцатеричное число 0x00.

Поясним значение элементов управления окна. В поле, расположенное ниже положения переключателя **Записать число**, вы можете ввести произвольное шестнадцатеричное число для записи его на произвольном проходе жесткого диска (в данном случае — на 1-м проходе).

Установив переключатель в положение **Записать случайное число**, вы, во-первых, тем самым выберете для записи на диск случайное число, во-вторых, сможете в поле ниже (спинере) указать длину случайного числа в байтах.

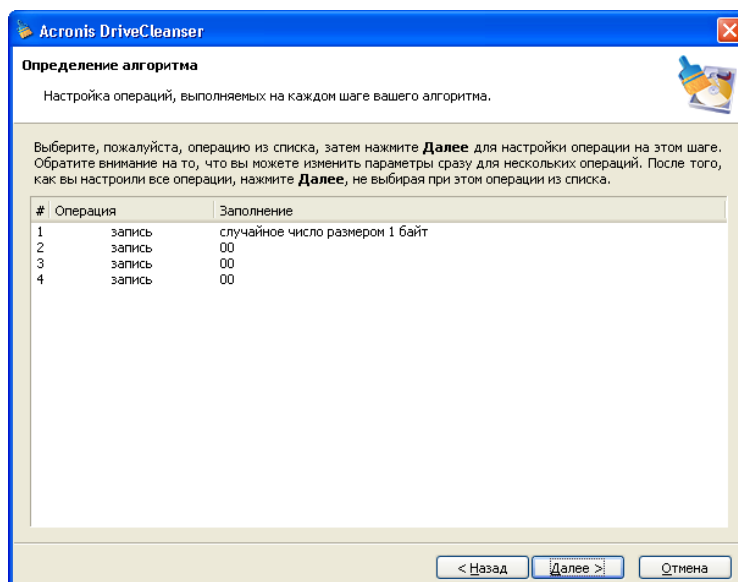
Американский национальный стандарт как раз предусматривает во время первого прохода диска запись случайных чисел в каждый байт каждого сектора, поэтому вы должны установить переключатель в положение **Записать случайное число** и ввести в поле значение, равное 1.



### Ввод в качестве образца для записи случайного числа длиной 1 байт

Для продолжения работы нажмите кнопку **Далее**.

Вы снова попадете в окно шаблона алгоритма и сможете увидеть, что прежняя запись («1 – запись – 00») сменилась на «1 – запись – случайное число размером 1 байт».



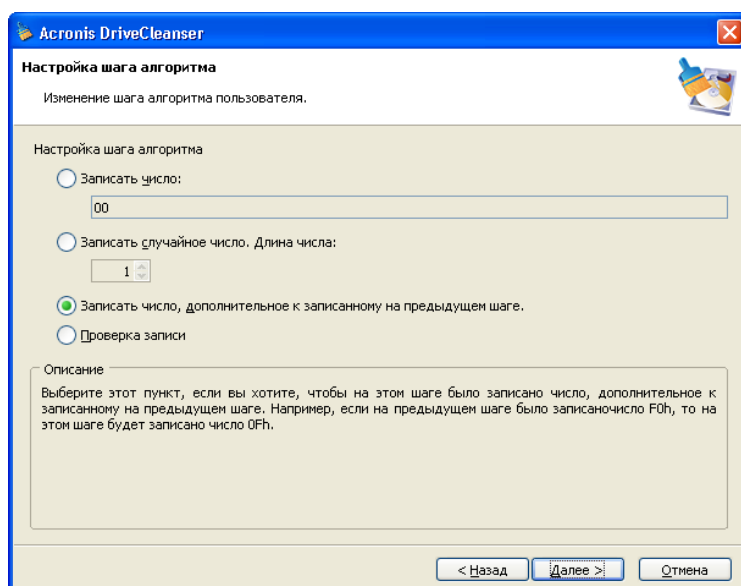
### Определен 1-й шаг пользовательского алгоритма

Для определения следующего прохода выделите вторую строку в списке и нажмите кнопку **Далее**.

Вы попадете в окно, уже знакомое вам, но на этот раз в нем вам будет доступно большее число положений переключателя: доступны для выбора два дополнительных положения переключателя:

- **Записать дополнительный код числа, записанного на предыдущем шаге,**
- **Проверка записи.**

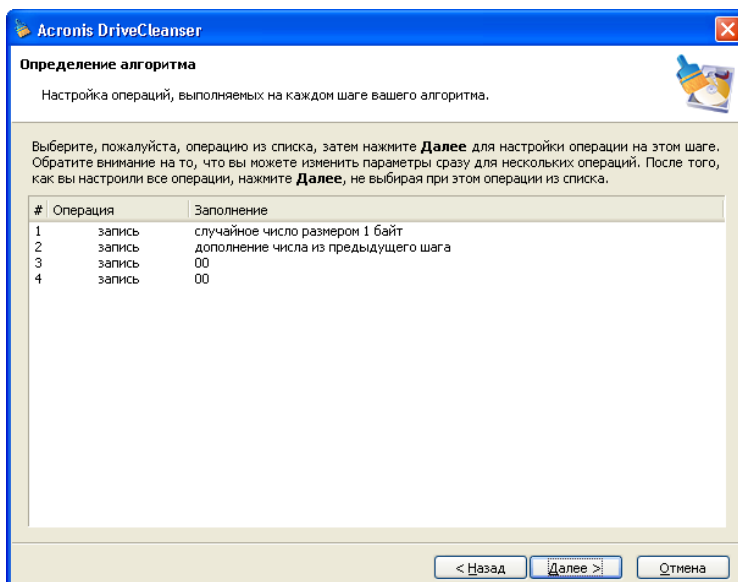
Эти положения логически имеют смысл, только после первого прохода по диску: до того, как осуществлен первый проход, бессмысленно выражение «предыдущий» и нечего, собственно говоря, проверять.



### Выбор числа, дополнительного к записанному на предыдущем шаге

Как вы помните, американский стандарт предусматривает во время второго прохода запись в каждый сектор диска шестнадцатеричных чисел, дополнительных к записанным на предыдущем проходе. Поэтому на этот раз в этом окне вам предлагается выбрать положение переключателя **Записать дополнительный код числа, записанного на предыдущем шаге** и нажать кнопку Далее.

Вы вновь попадете в окно шаблона алгоритма. В этом окне 2-я запись, прежде имевшая вид: «1 – запись – 00», сменилась на: «1 – запись – дополнительный код числа из предыдущего шага».



### Определен 2-й шаг пользовательского алгоритма

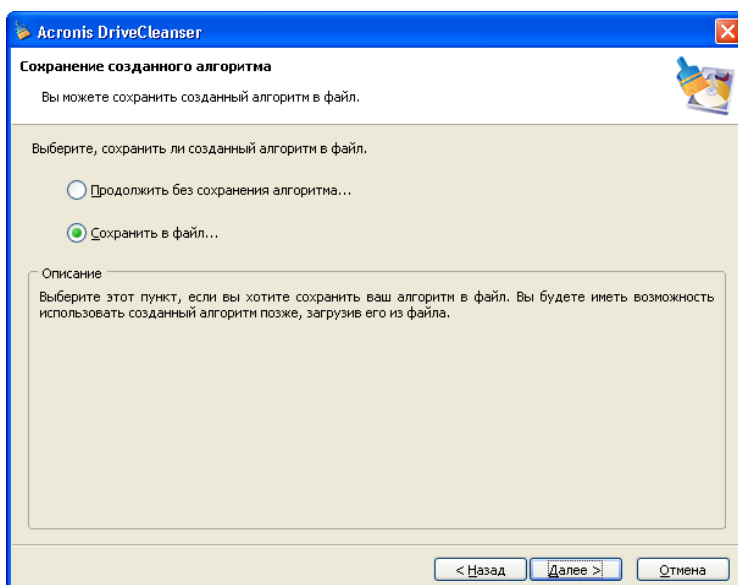
Аналогичным образом, следуя спецификации американского стандарта, создаем 3-й и 4-й проходы перезаписи жесткого диска.

Стоит отметить, что таким образом вы можете создать любой алгоритм, соответствующий вашим требованиям к безопасности.

### Сохранение пользовательского алгоритма в файле

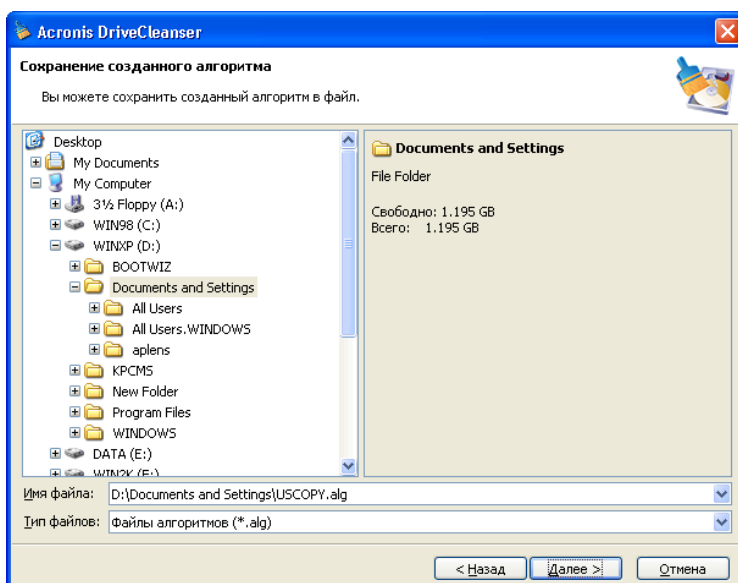
В следующем окне **Сохранение пользовательского алгоритма** вы можете сохранить алгоритм на диске в файле. Это может быть полезно, если вы собираетесь использовать созданный алгоритм в дальнейшем.





### Окно Сохранение пользовательского алгоритма

Для сохранения алгоритма в следующем окне введите имя файла, в котором будет храниться алгоритм, вместе с путем к нему в соответствующее поле или найдите существующий файл на диске.

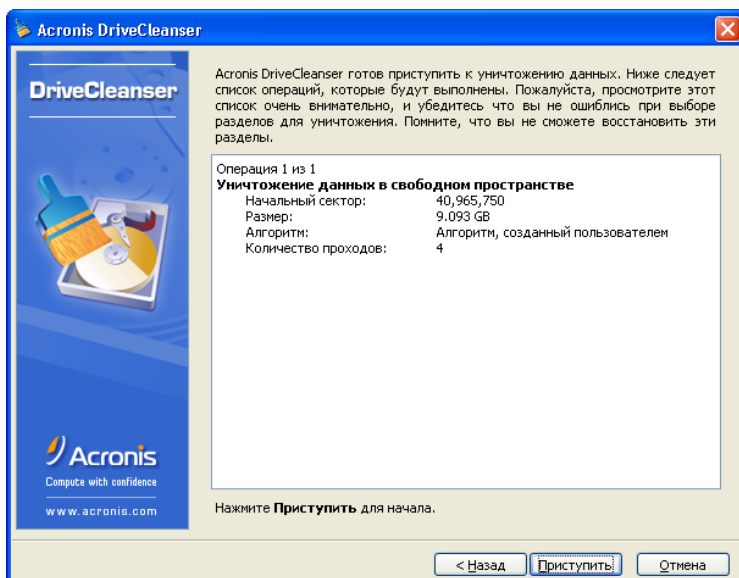


### Окно Имя файла и описание алгоритма



Каждый пользовательский алгоритм сохраняется в отдельном файле со своим именем. Если вы попытаетесь записать новый алгоритм в уже существующий файл, то его содержание будет затерто.

Таким образом, все проходы алгоритма определены, сам алгоритм сохранен в файле, так что, нажав на кнопку **Далее**, вы попадете в окно сформированного сценария уничтожения информации, основанного на вашем алгоритме.



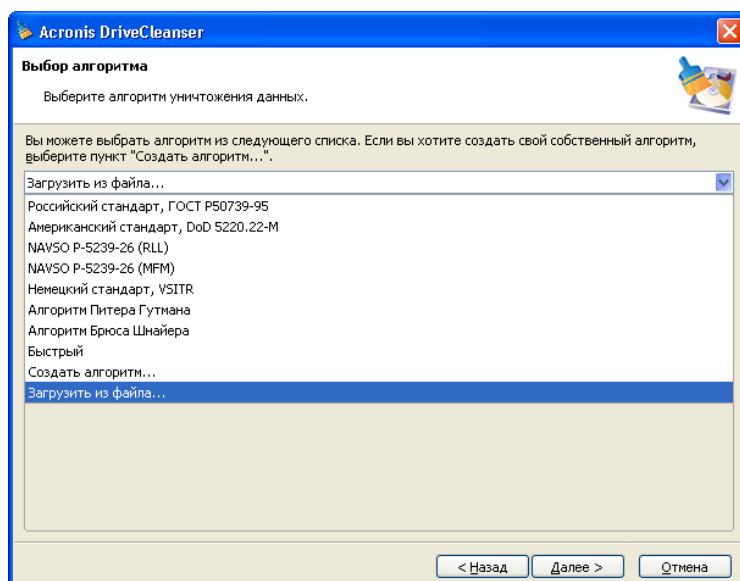
### Сценарий уничтожения информации, основанный на пользовательском алгоритме

Нажав на кнопку **Приступить**, вы тем самым запустите сформированный сценарий на выполнение.

### Загрузка алгоритма из файла

Если во время работы с программой Acronis DriveCleanser вы создали и сохранили на диске (в файлах) собственные алгоритмы уничтожения конфиденциальной информации, то воспользоваться ими вы можете следующим образом.

В окне **Выбор алгоритма** выберите в развертывающемся списке строку **Загрузить из файла...**



**Выбор пользовательского алгоритма: загрузка из файла**

# Приложение А. Алгоритмы уничтожения данных

## Необходимость специальных алгоритмов уничтожения информации

Информация, удаленная с жесткого диска неспециальными средствами (например, средствами операционной системы Windows) может быть легко восстановлена. При наличии специализированного оборудования возможно восстановление даже многократно перезаписанной информации. Поэтому сегодня проблема гарантированного уничтожения данных стоит как никогда остро.

Под **гарантированным уничтожением информации** на магнитных носителях понимается невозможность ее восстановления квалифицированными специалистами с помощью любых известных устройств и способов реставрации.

Пояснить существующую проблему можно следующим образом. Как известно, информация на жестком диске хранится в двоичной форме — в виде последовательности 1 и 0 (единиц и нулей), которые представляются различным образом намагниченными участками поверхности магнитного носителя.

Условно говоря, 1 записанная на жесткий диск, будет прочитана контроллером жесткого диска как 1, а записанный 0 будет прочитан как 0. Однако если поверх 0 будет записана 1, то результат, условно говоря, будет равен 0,95 и, наоборот, если поверх 1 будет записана 1, результат будет равен 1,05. Для контроллера эти различия совершенно несущественны. Но, используя специальную аппаратуру, легко прочитать, какую последовательность 1 и 0 содержала «нижележащая» запись.

Прочесть «стертые» таким образом данные можно используя специальные программные средства и недорогую аппаратуру, анализируя намагниченность секторов жесткого диска, остаточную намагниченность на краях дорожек, наконец, используя современные магнитные микроскопы.

Запись на магнитных носителях приводит к тонким эффектам, резюмировать которые можно так: каждая дорожка магнитного диска содержит **образ каждой записи (!)**, когда-либо сделанной на ней, но вклад каждой такой записи (магнитного слоя) тем меньше, чем раньше была сделана запись.

## Принцип действия алгоритмов уничтожения информации

Физически задача полного уничтожения информации на жестком диске сводится к тому, чтобы обеспечить перенамагничивание каждого элементарного магнитного участка записываемого материала как можно больше раз записью в сектора специально подобранных последовательностей логических 1 и 0 (образцов).

Используя знания о способах кодирования данных в современных жестких дисках, можно выбрать **образцы** записываемых в сектора последовательностей символов (или элементарных бит информации), чтобы **многократно и надежно затереть конфиденциальную информацию**.

Алгоритмы, предлагаемые национальными стандартами, предусматривают запись (одно-трехкратную) случайных символов в сектора диска, что является **прямолинейным и, в общем, произвольным решением**, приемлемым, однако, в простых ситуациях. Максимально надежный алгоритм уничтожения информации основывается на глубоком изучении тонких особенностей записи информации на жестких дисках всех типов. Именно знание этих особенностей диктует необходимость создания сложных многопроходных алгоритмов **гарантированного** уничтожения информации.

Подробное изложение теории гарантированного уничтожения информации можно найти, например, в статье Питера Гутмана (Peter Gutmann):

[http://www.cs.auckland.ac.nz/~pgut001/pubs/secure\\_del.html](http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html).

## Алгоритмы, используемые Acronis DriveCleanser

В таблице, приведенной ниже, кратко характеризуются алгоритмы уничтожения информации, используемые программой Acronis DriveCleanser. Для каждого алгоритма в таблице приведено количество проходов по секторам жесткого диска и записываемые в каждый байт сектора числа.

**Таблица 1. Описание встроенных алгоритмов уничтожения информации**

№№	Алгоритм (метод записи)	Количество проходов	Запись
1.	Американский: DoD 5220.22-M	4	1-й проход — случайно выбранные символы в каждый байт каждого сектора, 2 — дополнительные к записанным на 1-м проходе; 3 — снова случайно выбранные символы; 4 — верификация записей.
2.	Американский NAVSO P-5239-26 (RLL)	4	1-й проход — 0x01 во все сектора, 2 - 0x27FFFFFF, 3 — случайные последовательности символов, 4 — верификация.
3.	Американский NAVSO P-5239-26 (MFM)	4	1-й проход — 0x01 во все сектора, 2 - 0x7FFFFFFF, 3 — случайные последовательности символов, 4 — верификация.

№№	Алгоритм (метод записи)	Количество проходов	Запись
4.	Немецкий: VSITR	7	1-й — 6-й запись чередующихся последовательностей вида: 0x00 и 0xFF; 7-й - 0xAA; то есть 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.
5.	Российский: GOST P50739-95	1	Запись логических нулей (чисел вида 0x00) в каждый байт каждого сектора для систем с 6-го по 4-й класс защиты.  Запись случайно выбранных символов (чисел) в каждый байт каждого сектора для систем с 3-го по 1-й класс защиты.
6.	Алгоритм П. Гутмана	35	Алгоритм Питера Гутмана является очень сложным и основывается на разработанной им теории уничтожения информации на жестких дисках (см. <a href="http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html">http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html</a> ).
7.	Алгоритм Б. Шнайера	7	В своей книге «Прикладная криптография» Брюс Шнайер предложил алгоритм, состоящий из 7 проходов по диску: 1-й проход – запись логических единиц (0xFF), 2-й – нулей (0x00), 3-7 – случайно выбранных чисел.
8.	Быстрый	1	Запись логических нулей (чисел вида 0x00) во все очищаемые сектора.