ОРИГИНАЛЬНАЯ СТАТЬЯ

УДК 004.056.2(045)


# Методы уничтожения данных с жесткого диска

***Алена Алексеевна Жилина,*** *студентка факультета прикладной математики и информационных технологий, Финансовый университет, Москва, Россия*
***Alena A. Zhilina,*** *student, Faculty of Applied Mathematics and Computer Science, Financial University, Moscow, Russia*
*alen.zhilina@yandex.ru*

**АННОТАЦИЯ**

*В части защиты информации нередко возникают экстренные ситуации, когда лучшей защитой конфиденциальных данных является их полное уничтожение. Если говорить о таких носителях информации, как жесткие диски, большинство классических способов программного уничтожения данных не дает гарантии того, что информацию невозможно будет восстановить. Способы механического уничтожения информации, в свою очередь, требуют дополнительного оборудования и часто могут быть опасными для сотрудников (операторов), проводящих данную процедуру. Кроме того, во всех случаях качественное стирание данных требует относительно большого количества времени. В этой связи как наиболее эффективные на первое место выходят способы уничтожения информации аппаратными средствами. В данной статье рассматриваются существующие способы стирания информации с жестких дисков в целом, в частности остановиться на физических основах этого процесса и соответственно аппаратном уничтожении информации, провести сравнительную характеристику наиболее известных устройств, предназначенных для аппаратного уничтожения, а также продемонстрировать на практике работу с одним из таких устройств.*
***Ключевые слова:*** *жесткий магнитный диск; уничтожение данных; программные средства; магнитная индукция; напряженность электромагнитного поля; аппаратные средства; Samurai X-LITE; Прибой; Импульс; защита данных*

***Для цитирования:*** **Жилина А. А. Методы уничтожения данных с жесткого диска.** ***Научные записки молодых исследователей.*** **2020;8(4):65-73.**

ORIGINAL PAPER

# Hard Drive Data Erasure

**ABSTRACT**

*In the field of protection of information frequently occur, such emergencies in which the best option to protect the data is to erase it completely. Considering such data carries as hard drives, the majority of standard methods of program erasure does not guarantee that the information would be impossible to restore. Mechanical*

*Научный руководитель:* ***Егоров Е.В.,*** *старший преподаватель кафедры «Информационная безопасность», Финансовый университет, Москва, Россия / Scientific supervisor:* ***Egorov E.V.,*** *Senior Lecturer at the Department of Information Security, Financial University, Moscow, Russia.*

*methods of data erasure, on the other hand, require additional equipment and often can be dangerous for workers (operators) who conduct this procedure. Moreover, high-quality data erasure in all cases requires a relatively large amount of time. Therefore, the hardware method comes as the most effective method of data erasure. In this article I'd like to consider existing methods of hard drive data destruction as a whole, in particular — the physical basis of this process and, after that, hardware data erasure, to give a comparative description of the most widespread devices, and also to demonstrate how one of such devices operates.*
***Keywords:*** *magnetic hard drive; data erasure; software methods; magnetic induction; electromagnetic field strength; hardware methods; Samurai X-LITE; Priboy; Impulse; protection of information*

***For citation:*** **Zhilina A. A. Hard drive data erasure.** ***Nauchnye zapiski molodykh issledovatelei = Scientific notes of young researchers*****. 2020;8(4):65-73.**

## Введение

Потребность в системах хранения данных продолжает расти. В настоящее время выбор крупных компаний все чаще падает на облачные решения. Растущий спрос на системы хранения обусловлен также и приложениями, которые используются в новых областях, таких как анализ больших данных, в том числе для нейронных сетей, системы устройств интернета вещей. Более мелкие компании крупного и среднего бизнеса используют при работе большие массивы фотографий и видео, коммерческих данных и файлов крупных проектов.

Согласно прогнозам IDC с 2018 по 2025 г. общая емкость систем хранения, поставляемых на рынок, превысит 22 зеттабайт. 26% этого объема будет обеспечена флеш-устройствами. Но доля жестких дисков будет куда выше — 59%. Учитывая растущую популярность приложений с ИИ и инновационных служб автоматизации с поддержкой нового стандарта — 5G, предприятия и операторы центров обработки данных должны рассматривать все возможные варианты их хранения. В этой связи можно говорить о том, что популярность использования накопителей как части систем хранения, и в частности жестких дисков, в ближайшие годы будет только возрастать [1].

В данной статье:

- рассмотрены способы стирания информации с жестких дисков, а также выявлены наиболее эффективные из них;
- выведена формульная связь между понятиями индукции и индуктивности для элемента внешнего воздействия на жесткий диск;
- на практике рассмотрена работа Samurai X-LITE, соотнесены его технические характеристики с формульной зависимостью приведенных величин.

## Работа HDD. Индукция и индуктивность: связь понятий

Для осуществления записи данных на жестких дисках используется магнитная головка жесткого диска (*рис. 1*). Она состоит из двух частей: головки чтения и головки записи. Работа головки чтения заключается в определении изменений магнитного потока, которые модулируют нулевой и единичный биты. Головка записи имеет более сложную конструкцию, поскольку ей нужно создавать достаточно сильное магнитное поле, чтобы менять ориентацию магнитных доменов в пластине. Для данной задачи используется одна или большее число катушек.

При подаче переменного электрического тока (во время записи) на катушку головки возникающее переменное магнитное поле из зазора головки воздействует на ферромагнетик поверхности диска и изменяет направление вектора намагниченности доменов в зависимости от величины сигнала. При считывании перемещение доменов у зазора головки приводит к изменению магнитного потока в магнитопроводе головки, что приводит к возникновению переменного электрического сигнала в катушке за счет электромагнитной индукции[1].

Для размагничивания жесткого диска необходимо воспользоваться свойствами магнитного гистерезиса, по графику которого и происходит намагничивание, а именно коэрцитивной силой, означающей напряженность магнитного поля, в котором ферромагнитный образец, первоначально намагниченный до насыщения, размагничивается.

Из формулы напряженности видим, что коэрцитивная сила в данном случае зависит от магнитной индукции головки жесткого диска:

[1] Жесткий диск. URL: https://ru.wikipedia.org/wiki/Жесткий_диск (дата обращения: 29.01.2020).

$$H = B/\mu_0, \quad (1)$$

где $H$ — напряженность магнитного поля; $\mu_0$ — магнитная проницаемость среды; $B$ — магнитная индукция головки.

Учитывая значение

$$\mu_0 = 4\pi \times 10^{-7}\, H/A^2 = 12{,}56 \times 10^{-7}\, H/A^2,$$

можно говорить о том, что коэрцитивная сила определяется величиной магнитной индукции головки жесткого диска, т.е. силовой характеристикой существующего вокруг нее магнитного поля. Соответственно, для размагничивания магнитной головки необходимо внешнее воздействие на нее электромагнитного поля силы, превышающей величину ее магнитной индукции.

В лабораторных условиях такое поле может быть создано внешней катушкой с подведенным к ней током. Магнитная индукция при этом должна определяться величиной индуктивности (для связи между электрическим током и магнитным потоком существует коэффициент пропорциональности, называемый индуктивностью) магнитной головки. Из документации по работе с жесткими дисками можно увидеть, что в среднем эта величина составляет 250–1000 мГн.

Для связи магнитной индукции и индуктивности необходимо использовать формулы магнитного потока. Тогда, с одной стороны:

$$\Phi = NBS\cos\alpha, \quad (2)$$

где Ф — магнитный поток; $N$ — число витков; $B$ — магнитная индукция; $\alpha$ — угол вектора индукции. С другой стороны:

$$\Phi = LI, \quad (3)$$

где $L$ — индуктивность; $I$ — ток, подводимый к катушке.

Приравняв правые части формул (2) и (3), получим:

$$L = \frac{NBS}{I} = [250 - 1000]\ \text{мГн}. \quad (4)$$

При использовании катушки из пяти витков площадью 0,5 см на 0,5 см можно свести формулу (4) к виду:

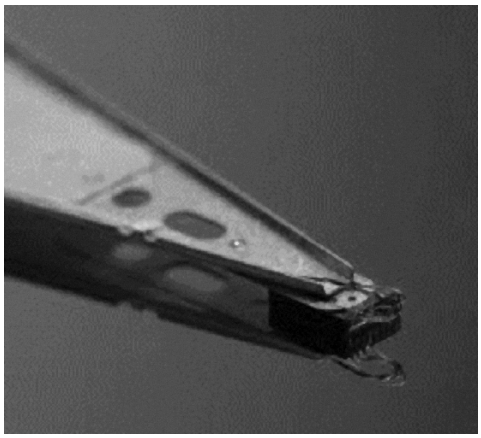

*Рис. 1.* ***Магнитная головка жесткого диска***

*Источник:* URL: https://helpiks.org/6–29815.html.

$$L = 0{,}039\frac{B}{I} = 0{,}49 \cdot 10^{-7}\frac{H}{I} = [250 - 1000]\ \text{мГн}. \quad (5)$$

Таким образом, для стирания информации аппаратным устройством остается подобрать напряженность магнитного поля и подводимый ток.

Рассмотрим теперь, какие существуют альтернативные способы уничтожения информации вообще.

## Методы уничтожения данных на жестких магнитных дисках

В общем случае все методы уничтожения данных на жестких магнитных дисках делятся на три группы: программные, механические и аппаратные.

В основу программных методов положено использование штатных средств записи информации на магнитных носителях. После использования данного метода носитель может быть повторно использован в других персональных компьютерах (ПК), после инсталляции новой операционной системы (ОС) и приложений. Уничтожение производится полной или частичной перезаписью диска. При перезаписи информации работоспособность жесткого диска полностью сохраняется.

Механические методы связаны с механическим повреждением основы, на которую нанесен магнитный слой — физический носитель информации.

### Программные методы уничтожения данных

Оба алгоритма перезаписи диска сводятся к $N$-кратному форматированию и записи на него двоичных единиц, нулей и псевдослучайных чисел. Основным минусом данного метода считается скорость его работы. Так, информация с диска объемом в 500 Гб будет «стираться» около 13 часов.

*Таблица 1*

**Классификация аппаратных средств уничтожения информации**

| Признак | Виды программных средств |
|---|---|
| Принцип действия | С плоской катушкой |
| | С объемным соленоидом |
| По месту размещения | В корпусе ПК |
| | В корпусе корпоративного сервера |
| | В корпусе переносного кейса для хранения жесткого диска |
| | В корпусе офисного сейфа |
| | Плановые утилизаторы (представляет собой отдельно стоящее устройство) |

*Источник:* составлено автором.

• Полная перезапись диска может быть выполнена встроенными командами определенной операционной системы. Для ОС Windows — format c:, где «c:» — имя логического раздела, для Unix-подобных ОС: «dd if=/dev/zero of=/dev/sda bs=4k», где «/dev/sda» — адрес устройства для форматирования.

Частичная перезапись данных происходит псевдослучайными числами через API драйвера диска при наличии прямого подключения к жесткому диску. В этом случае также есть возможность получения адресов, в которых хранится информация, и перезаписывать только эту область памяти[2].

**Механические методы уничтожения данных**

С.Р. Коженевский выделял следующие методы уничтожения информации, предполагающие механическое воздействие [2]:

• Механическое воздействие предполагает измельчение носителя так, чтобы исключить возможность прочтения информации каким-либо способом с его рабочих дисков [например, используя устройство измельчения (шредер)].

Указанный метод не исключает возможности восстановления информации по фрагментам в лабораторных условиях. Также существует опасность повреждения пластин жесткого диска и выводу его из строя. К примеру, пыль стирает рабочий слой до основы уже через несколько часов работы с вскрытой гермокамерой.

Часто используемые на практике методы сверления отверстий и удары молотком по приводу на самом деле вовсе не уничтожают или уничтожают только малую часть информации.

• Термический представляет собой метод нагревания носителя до температуры плавления в специальных печах.

Гарантия полного уничтожения информации появляется при нагревании носителя в диапазоне температуры от 800 до 1000 °С. При такой температуре магнитный материал рабочего слоя переходит через точку Кюри.

• Пиротехнический является методом разрушения носителя посредством взрыва. Предполагает опасность для оператора.

• Металлотермический метод предполагает уничтожение подложки диска с магнитным покрытием высокой температурой самораспространяющегося высокотемпературного синтеза (СВС). При этом на подложку в процессе производства наносится специальный слой термитного покрытия.

• Химический метод представляет собой разрушение рабочего слоя или основы носителя химически агрессивными средами.

При использовании данного метода имеет место проблема обеспечения безопасности оператора.

*Рис. 2.* ***2С-994 «Прибой». Внешний вид***

*Источник:* URL: https://www.ixbt.com/storage/hddterminator.shtml.

[2] Как стереть данные так, чтобы их не смогли восстановить спецслужбы? URL: https://habr.com/ru/company/storelab/blog/151554/ (дата обращения: 30.01.2020).

• Радиационный метод предполагает разрушение носителя ионизирующими излучениями. Могут быть экологически небезопасными, в противном случае не обеспечивают высокую надежность уничтожения информации, при этом требуют специфического и дорогостоящего оборудования.

Существует опасность облучения для оператора.

Во всех механических методах отсутствует возможность повторного использования накопителей на жестких магнитных дисках (НЖМД).

**Аппаратные методы уничтожения данных**

Данный класс методов можно классифицировать по нескольким признакам. Проведем классификацию по принципу действия средства и по месту его размещения относительно носителя информации (*табл. 1*).

Значительно более перспективным следует признать применение для уничтожения информации кратковременно создаваемого мощного электромагнитного поля. В нашем случае сила такого воздействия есть сила магнитной индукции внешнего поля, которым производится воздействие на пишущую головку.

Такой способ стирания записей за счет намагничивания носителя импульсным магнитным полем определенной величины и ориентации запатентован отечественными специалистами [3].

## Аппаратные средства уничтожения информации «Прибой», «Samurai X-Lite», «Импульс». Сравнительная характеристика

Основными из известных устройств стирания записей за счет такого намагничивания являются 2С-994 «Прибой», SAMURAI X-LITE, Импульс-7В. Внешний вид приборов представлен на *рис. 2–4*. Принцип их действия аналогичен действию внешнего магнитного поля, создаваемого магнитными головками при записи. Когда напряженность внешнего поля превышает величину магнитного насыщения материала поверхности диска жесткого диска, все магнитные домены поверхности жесткого диска гарантированно переориентируются по направлению внешнего поля, и вся информация с жесткого диска экстренно безвозвратно уничтожается [4].

Приведем краткую характеристику и сферу применения каждого из устройств и далее рассмотрим их в сравнении (*табл. 2*).


*Рис. 3.* ***Samurai X-Lite. Внешний вид***

*Источник:* URL: https://www.samurai24.ru/catalog/zashhita-pk/zashhita-pk-samurai-x-lite.html.

*Рис. 4.* ***Импульс-7В. Внешний вид***

*Источник:* URL: informacii/dlya-pk-i-noutbukov/impuls_5v_na_1_disk_dlya_pk/.

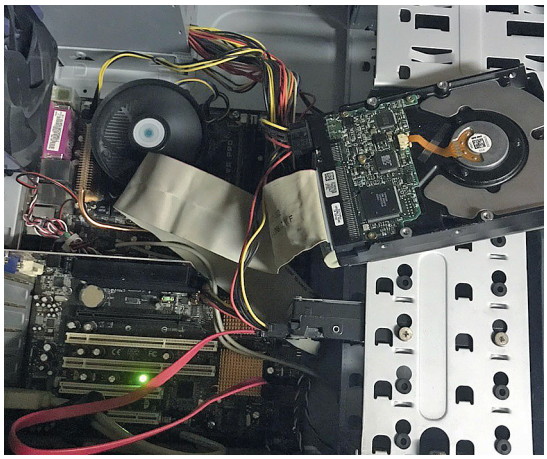

*Рис. 5.* ***Подключение жесткого диска к компьютеру***

*Источник:* фото автора.

По характеристикам приведенных выше устройств была составлена сравнительная *табл. 3*.

Из *табл. 3* видно, что наиболее мощным, а также подходящим под максимальное количество возможных ситуаций является устройство Импульс-7В. Для проведения практической части данной работы был выбран SAMURAI X-LITE как устройство, обладающее средними характеристиками.

*Таблица 2*

**Характеристика аппаратных средств уничтожения информации**

| Наименование и производитель | Описание | Лицензирование |
|---|---|---|
| 2С-994 «Прибой» ООО «Компьютерные сервисные устройства» (КСУ) | Предназначено для защиты отдельных рабочих мест, где осуществляется работа с данными (за исключением данных, относящихся к сведениям государственной тайны). Изделие способно оперативно удалить информацию, выводя при этом из строя установленный в ПК жесткий диск по команде пользователя либо при постороннем доступе | Компания имеет лицензии Гостехкомиссии России, Министерства обороны РФ на деятельность в области разработки и производства средств защиты информации. Производство устройств уничтожения данных имеет заключение по системе качества ISO-9001* |
| SAMURAI X-LITE Samurai24 | Представляет собой упрощенную систему уничтожения данных для самостоятельной установки в корпус ПК для уничтожения одного диска. Устройство устанавливается в отсек как CD-ROM. Жесткий диск, нуждающийся в защите, устанавливается прямо под устройство Samurai X-Lite в специальные салазки** | – |
| Импульс-7В ООО «Детектор Системс» | Может применяться как в случаях необходимости экстренного уничтожения ценной информации (конфиденциальных данных), так и при списании информационных носителей | Компания имеет лицензии ФСТЭК и ФСБ на деятельность, связанную с государственной тайной, лицензию ФСТЭК по технической защите конфиденциальной информации, сертификат соответствия ISO 9001:2015*** |

*Источник:* составлено автором.

* «Прибой» свой жесткий диск. URL: https://www.ixbt.com/storage/hddterminator.shtml (дата обращения: 03.02.2020).
** ЗАЩИТА ПК SAMURAI X-LITE. URL: https://www.samurai24.ru/catalog/zashhita-pk/zashhita-pk-samurai-x-lite.html (дата обращения: 04.02.2020).
*** Импульс-7В. URL: https://detsys.ru/catalog/ustrojstva-unichtozheniya-informacii/dlya-pk-i-noutbukov/impuls_5v_na_1_disk_dlya_pk/ (дата обращения: 04.02.2020).

## Применение Samurai X-LITE на практике. Опыт по проверке рассчетного значения

Имея технические характеристики Samurai X-Lite, можем подставить значение напряженности (450 кА/м) в формулу (5). Выразим и рассчитаем значение тока при индуктивности $L$ = 1 Гн:

$$I = 0,49 \cdot 10^{-7} \cdot 450 \cdot 10^{3} = 0,2205\ A. \qquad (6)$$

Таким образом, мы получаем реальное значение тока для устройства уничтожения информации с жесткого диска.

В ходе проведения опыта с устройством Samurai X-Lite был выбран жесткий диск в рабочем состоянии и предварительно проверена корректность его работы при подключении к ПК.

На *рис. 5* показано стандартное подключение испытуемого жесткого диска по IDE интерфейсу к материнской плате и блоку питания, а на *рис. 6*

*Рис. 6.* ***Работа жесткого диска до воздействия Samurai X-Lite***

*Источник:* фото автора.

*Рис. 7.* ***Работа Samurai X-Lite***

*Источник:* фото автора.

*Таблица 3*

**Сравнительная характеристика устройств уничтожения информации**

| | 2С-994-В «Прибой» | SAMURAI X-LITE | Импульс-7В |
|---|---|---|---|
| Возможность восстановления информации | Отсутствует | Отсутствует | Отсутствует |
| Распознавание жесткого диска после использования | Отсутствует | Отсутствует | Отсутствует |
| Размер разъема для жесткого диска, дюйм | 3,5 | 3,5 | 3,5 / 2,5 / 1,8 |
| Тип питания | От сети | От блока питания компьютера | От аккумулятора |
| Способ уничтожения данных | Скрытая кнопка, пульт-передатчик к радиоблоку | Скрытая кнопка | Проводные кнопки, радиоканал, бесконтактные ключи, лвс модуль активации |
| Радиус действия передатчика (при наличии), м | 100 | – | Для кнопок: 100, для радиоканала: 1000 |
| Напряженность питания, В | 12 | 12...14 | 12 |
| Напряженность э/м поля при срабатывании, кА/м | 450 | 450 | 500 |
| Максимальное время зарядки силового блока, сек | 180 | 10 | 60 |
| Стоимость, руб. | 18.000–22.000 | 21.000 | 34.000 |

*Источник:* составлено автором.

представлен экран загрузки с этого диска (с установленной системой Windows 7).

Далее жесткий диск был помещен в специальные салазки устройства Samurai X-LITE, как показано на *рис. 7*, затем с помощью ручки была нажата скрытая кнопка для срабатывания системы.

После описанных действий при повторном подключении к компьютеру жесткого диска носитель не был распознан компьютером как запоминающее устройство, что продемонстрировано на *рис. 8*.

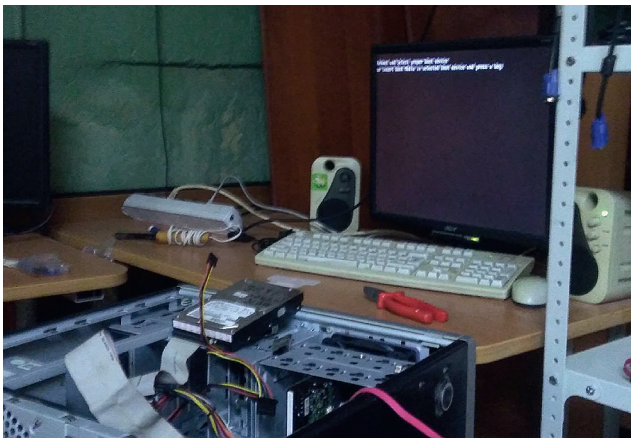

*Рис. 8.* ***Работа жесткого диска после воздействия Samurai X-LITE***

*Источник:* фото автора.

## Проблемы и перспективы развития жестких дисков в различных сферах

### Альтернативные способы хранения данных

Механический накопитель на жестких дисках (HDD) был стандартом систем хранения для компьютеров по всему миру в течение более 30 лет. Однако в настоящее время наряду с жесткими дисками используются и другие способы хранения данных, такие как флеш-накопители и внешние SSD-диски. Возникает вопрос об области использования каждого из видов накопителей, их преимуществах и недостатках в сравнении друг с другом. Рассмотрим каждое из устройств по данным параметрам (*табл. 4*) [5].

Как было отмечено выше, SSD-диски являются лидерами по скорости среди носителей[3]. Соотношение между скоростями SSD- и жестких дисков можно увидеть на *рис. 9*. Здесь используется бен-

[3] Флеш-накопитель USB против внешнего жесткого диска и SSD: в чем различие? URL: https://zen.yandex.ru/media/comphit/fleshnakopitel-usb-protiv-vneshnego-jestkogo-diska-i-ssd-v-chem-razlichie-5dff86cdc31e4900b580dd52 (дата обращения: 04.02.2020).

*Таблица 4*

**Преимущества и недостатки альтернативных устройств хранения информации**

| Вид | Преимущества | Недостатки |
|---|---|---|
| Флеш-накопители | 1. Компактность.<br>Использование флеш-накопителей является наиболее удобным вариантом для хранения и частого переноса информации.<br>2. Прочность.<br>Данный вид накопителя обладает компактностью и не имеет движущихся частей, что делает их устойчивыми к ударам и практически исключает возможность поломки или износа | 1. Сравнительно небольшой объем памяти.<br>В среднем используются накопители на 8–16 Гб. Максимальный объем памяти составляет 256 Гб (Samsung).<br>2. Стоимость.<br>Обычно в 8–10 раз дороже жестких дисков с аналогичными характеристиками. Однако такая разница вполне оправданна, если речь идет о загрузочном устройстве для сервера или приложения уровня tier-0, так что вряд ли жесткие диски вновь займут эту нишу |
| SSD-накопители | 1. Скорость.<br>SSD-диски не имеют в конструкции движущихся частей, что существенно повышает их скорость работы. В отличие от жестких дисков для хранения и записи информации используется полупроводниковый принцип.<br>2. Надежность.<br>Ввиду отсутствия механических частей являются менее чувствительными к ударам и сотрясениям | 1. Стоимость.<br>В данный момент этот вид носителя является наиболее дорогостоящим.<br>2. Ограничение по количеству циклов перезаписи |
| Жесткие диски | 1. Срок службы.<br>В среднем составляет порядка 10 лет, в отличие от SSD, срок жизни которого зависит от количества циклов перезаписи.<br>2. Стоимость.<br>При сравнении накопителей большего объема жесткие диски заметно выигрывают в стоимости у других накопителей, обладающих такими же характеристиками | Производительность |

*Источник:* составлено автором.

чмарк CrystalDiskMark для оценки жесткого диска WD 3.5» 5400 RPM 2 TB.

В первых двух строчках указано количество МБ в секунду при выполнении последовательных (длинный, непрерывный список) и случайных (переходы по всему накопителю) чтения и записи. В следующей строке показано значение IOPS, т.е. количество операций ввода-вывода, выполняемых каждую секунду. В последней строке показана средняя задержка (время в микросекундах) между передачей операции чтения или записи и получением значений данных.

Из *табл. 4*, а также из приведенной выше оценки скоростей можно сделать вывод о том, что основным конкурентом для жестких дисков среди устройств хранения данных являются SSD по скорости работы и производительности. Однако согласно результатам исследования, проведенного компанией Toshiba, решения с большим количеством жестких дисков в конфигурации RAID 10 или с программно-определяемой архитектурой для параллельных вычислений превосходят решения на базе нескольких твердотельных накопителей той же стоимости по количеству операций ввода-вывода в секунду (для блоков данных размером более 64 Кбайт) и при этом обеспечивают втрое большую емкость.

Таким образом, многодисковые решения с подходящей конфигурацией могут составить хорошую альтернативу как флеш-накопителям, так и SSD[4].

[4] Что выбрать в 2019 году SSD или HDD? Разберем все плюсы и минусы. URL: https://zen.yandex.ru/media/techno_blog/chto-vybrat-v-2019-godu-ssd-ili-hddrazberem-vse-pliusy-i-minusy-5d8f2004fbe6e700adaa3c9a (дата обращения: 05.02.2020).

## Выводы

В заключение можно привести ряд рекомендаций для избегания компрометации конфиденциальных данных после их уничтожения:

- При недолговременном применении данных можно использовать энергозависимую (оперативную) память. В этом случае уничтожение не потребуется.
- При использовании других носителей, на которых когда-либо была записана копия конфиденциальной информации, необходимо убедиться в невозможности восстановления этих данных при помощи специальных программных средств.
- При передаче данных по сети рекомендуется использовать устройства криптографической защиты. При хранении конфиденциальной информации на сервере имеет смысл шифровать такую информацию с помощью специального ПО.

Развитие технологий ведет к росту объема передачи данных в секунду в пространстве данных. Производительность твердотельных накопителей

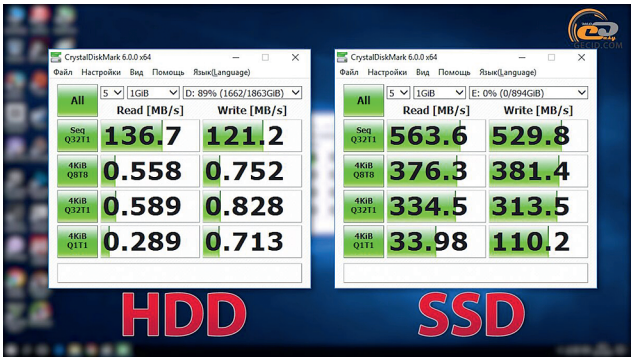


*Рис. 9.* ***Сравнение скоростей SSD и HDD (жесткого диска)***

*Источник:* URL: https://zen.yandex.ru/media/techno_blog/chto-vybrat-v-2019-godu-ssd-ili-hddrazberem-vse-pliusy-i-minusy-5d8f2004fbe6e700adaa3c9a.

идеально подходит для краткосрочного хранения данных интернета вещей. Но если говорить о долгосрочном хранении, аналитике и архивации, то здесь безоговорочно выигрывают жесткие диски и ленточные накопители — только они могут предоставить достаточную емкость.

## Список источников

1. Райнер В. Кезе. Перспективы использования жестких дисков в 2020 год. URL: https://www.it-world.ru/tech/science/151556.html (дата обращения: 04.02.2020).
2. Коженевский С. Методы гарантированного уничтожения данных на жестких магнитных дисках. URL: http://masters.donntu.org/2011/frt/riabtsev/library/article15.htm (дата обращения: 29.01.2020).
3. Болдырев А.И., Сталенков С.Е. Надежное стирание информации — миф или реальность? URL: http://masters.donntu.org/2011/frt/riabtsev/library/article4.htm (дата обращения: 01.02.2020).
4. Поздняков О. Как за секунды навсегда уничтожить данные с дисков и серверов. URL: https://zen.yandex.ru/media/id/5c766712fc48e500b1b3b96b/kak-za-sekundy-navsegda-unichtojit-dannye-s-diskov-i-serverov-5c77d03d08fe6800b464fac3 (дата обращения: 29.01.2020).
5. Evanson N. Anatomy of a Storage Drive: Hard Disk Drive. URL: https://www.techspot.com/article/1984-anatomy-hard-drive/ (дата обращения: 04.02.2020).

## References

1. Rainer V. Keze. Prospects for using hard drives in 2020 URL: https://www.it-world.ru/tech/science/151556.html (In Russ.).
2. Kozhenevsky S. Methods for guaranteed destruction of data on hard magnetic disks. URL: http://masters.donntu.org/2011/frt/riabtsev/library/article15.htm (In Russ.).
3. Boldyrev A.I., Shtalenkov S.E. Reliable erasing of information — myth or reality? URL: http://masters.donntu.org/2011/frt/riabtsev/library/article4.htm (In Russ.).
4. Pozdnyakov O. How to permanently delete data from disks and URL servers in seconds. URL: https://zen.yandex.ru/media/id/5c766712fc48e500b1b3b96b/kak-za-sekundy-navsegda-unichtojit-dannye-s-diskov-i-serverov-5c77d03d08fe6800b464fac3 (In Russ.).
5. Evanson N. Anatomy of a Storage Drive: Hard Disk Drives. URL: https://www.techspot.com/article/1984-anatomy-hard-drive/