УДК 343.98 + 004.43 Вестник УрФО № 2(32) / 2019, с. 12–17

Зулькарнеев И. Р., Карпов М. Г., Нестор В. О.

DOI: 10.14529/secur190202

ОСОБЕННОСТИ РАЗРАБОТКИ АППАРАТНОГО КРИМИНАЛИСТИЧЕСКОГО ДУБЛИКАТОРА ДАННЫХ НА БАЗЕ РАЗЛИЧНЫХ ИНТЕРФЕЙСОВ

В данной работе описываются особенности разработки аппаратного криминалистического дубликатора данных на основе интерфейсов взаимодействия с накопителями IDE и SATA. Рассматриваются проблемы, не позволяющие использовать единый подход для разработки прототипа устройства, и пути их решения. Произведен анализ и выбор аппаратных платформ с описанием их преимуществ для интерфейса SATA.

Ключевые слова: *компьютерно-техническая экспертиза, форензика, целостность, микроконтроллеры, дубликаторы данных, IDE, ATA, НЖМД, ПЛИС.*

Zulkarneev I. R., Karpov M. G., Nestor V. O.

SPECIFICITIES OF HARDWARE-FORENSIC DATA DUPLICATOR DEVELOPMENT BASED ON VARIOUS INTERFACES

The paper describes specificities of hardware-forensic data duplicator development on the basis of IDE u SATA drive interactive interfaces. Precluding problems of a unified approach usage to prototype such duplicator are examined. Solutions of these problems are proposed. The advantages of various platform usage for SATA interface described for choice making analysis.

Keywords: *computer forensic, integrity, microcontrollers, data duplicator, IDE, ATA, HDD, FPGA.*

Воспроизводимость исследований при производстве компьютерно-технических экспертиз (КТЭ) является одним из основополагающих требований, которое позволяет обеспечить объективность и достоверность экспертной работы [1]. Авторами ранее был предложен первый в России метод по реализации таких требований с использованием исключительно аппаратных средств.

Выполнение требований сохранения целостности в рамках проведения КТЭ может достигаться только при условии сохранения исходного состояния объекта исследования, представленном в виде цифровой информа-

ции, зафиксированном на машинном носителе.

При этом сохранение исходного состояния данных зависит не только от квалификации действий эксперта, но и от типа накопителя, который содержит исследуемые данные [2]. Относительно свойства состояния данных выделяют две группы накопителей:

• выполняющие динамическое преобразование данных;

• обеспечивающие контроль изменения данных.

Например, к первой группе относят полупроводниковые накопители, для которых сохранение целостности (СЦ) не представляется возможным ввиду технических особенностей их работы [3]. Во вторую группу входят магнитные и оптические носители данных. Однако, проблема технической неспособности осуществлять СЦ существует и для поврежденных или бывших в длительном использовании накопителей второй группы, которые в процессе работы осуществляют неконтролируемые изменения в содержащейся на них информации. Контроль данных в НЖМД осуществляется на уровне команд стандарта ATA.

С целью осуществления контроля СЦ целесообразно использовать аппаратное клонирование данных накопителя. Такой подход наиболее надежен с точки зрения минимизации рисков нарушения целостности данных [4, 5]. Однако, в настоящее время отсутствуют отечественные аппаратные устройства, обеспечивающие высокоскоростное копирование данных (до 9 ГБ/мин) между накопителями без угрозы нарушения целостности данных. В предыдущем исследовании авторами были изложены принципы, алгоритмы и требования к функционалу работы такого устройства - дубликатора [5]. В данной работе описываются условия разработки дубликатора, реализующего минимальный функционал, на базе различных аппаратных интерфейсов с целью выбора подходящего.

Дубликатор состоит из трех основных элементов: контроллера, двух накопителей и двух интерфейсов обмена данными. Основное управляющее устройство прототипа – контроллер Teensy 3.6 был выбран авторами ввиду наличия технических характеристик, удовлетворяющих выдвинутым требованиям [4, 5]. Принимая во внимания его параметры, было выполнено сравнение интерфейсов обмена данными группы ATA: Parallel-ATA и Serial-ATA (Таблица 1).

Таблица 1

Сравнение интерфейсов PATA и SATA

Характеристика	PATA	SATA
Максимальная скорость передачи данных	133 Мб/с	600 Мб/с
Максимальная частота шины	33 МГц	1500 МГц
Напряжение на пинах	+3,3 В	0,25 В
Тип сигнала	Постоянный	Дифференциальный
Количество пинов	39	4

Parallel-ATA (PATA или IDE) – параллельный интерфейс обмена данными. Обладает возможностью производить одновременное подключение двух накопителей. Максимальная скорость передачи данных - 133 Мб/с. Напряжение каждого пина данных – +3.3 V, питания – +5 V. Интерфейс PATA содержит 40 пинов [6].

Serial-ATA (SATA) – последовательный интерфейс обмена данными. Возможно подключение только одного накопителя. Максимальная скорость передачи данных – 600 Мб/с. Передача данных осуществляется по двум парам дифференциальных каналов напряжением 0,25 V. Частота шины достигает 1500 МГц [7].

Обмен данными между НЖМД и хостом по протоколу ATA осуществляется через десять регистров ввода\вывода. Регистр состояния устройства, регистр адреса накопителя являются системными, вследствие чего не используются для передачи данных. Оставшиеся восемь регистров — семь регистров для задания команды и чтения ответа от НЖМД и один регистр для передачи данных — используется в прототипе для копирования данных с исходного НЖМД на целевой при программировании контроллера.

При вызове определенной команды

НЖМД, требуется последовательно заполнить семь регистров необходимой информацией. Далее, для считывания ответа, требуется также прочитать информацию с семи регистров. В случае выполнения команды чтения данных, требуется лишь считать данные с нулевого регистра (см. рис. 1).

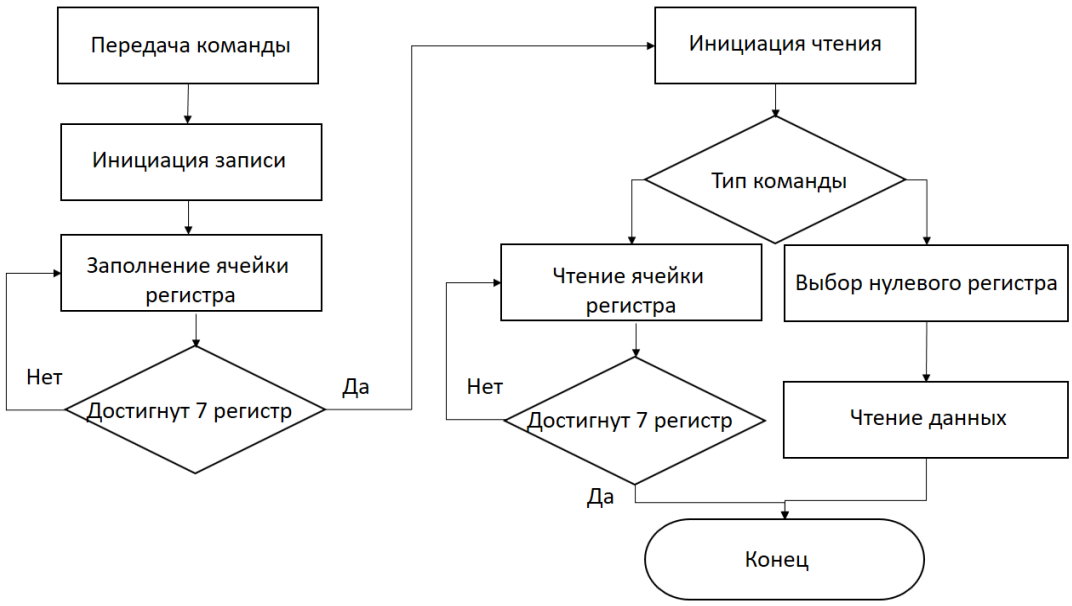

Рис 1. Схема копирования данных по интерфейсу ATA

Для взаимодействия с регистрами через интерфейс PATA требуется 23 пина: 5 пинов для выбора регистра, 16 пинов для передачи данных и 2 пина для переключения режимов чтения и записи. Помимо этого, для увеличения скорости чтения/записи данных, потребуется взаимодействие с режимом DMA, что потребует еще 2 пина. (см рис. 2).

Плата Teensy 3.6 толерантна к 3.3V логике и не имеет дифференциальных выводов, что делает невозможным ее взаимодействие с интерфейсом SATA. Следовательно, для целей реализации прототипа контроллер и накопители будут взаимодействовать через интерфейс IDE.

Частота процессора выбранного контроллера составляет 180 МГц, что делает невозможным осуществление быстрой передачи данных с его использованием – максимальная теоретическая скорость 180 Мб/сек. По этой причине при разработке прототипа в основу алгоритмов была положена идея zero-copy, которая минимизирует участие процессора в процессе копирования данных с одного накопителя на другой. Ее реализация состоит в использовании режима DMA. Плата Teensy 3.6 так же имеет аппаратную поддержку режима DMA, а ее программная составляющая реализуется логикой алгоритма.

Однако низкая тактовая частота микроконтроллера, а также дифференциальная передача низковольтных сигналов интерфейса SATA не позволяет работать с данным интерфейсом, из-за чего возникает проблема дальнейшего развития дубликатора данных на выбранной платформе с интерфейсом SATA [8]. Решение данной задачи возможно следующими путями:

• реализация системы на базе процессора Intel x86-64;

• использование программируемой логической интегральной схемы (ПЛИС).

Максимальной скорости передачи данных можно достичь, реализовав вышеописанный алгоритм на программируемой пользователем вентильной матрице (ППВМ), что является подвидом ПЛИС [9]. Микросхема ППВМ состоит из отдельно программируемых блоков, которые представляют из себя булеву функцию от шести аргументов и триггера. Булева функция задает таблицу истинности от аргументов, а триггер управляет выходным сигналом и подает его либо синхронно (в соответствии с тактовым генератором), либо асинхронно.

Основное преимущество ППВМ, перед выбранным микроконтроллером, состоит в более высокой скорости обработки данных. При работе с ППВМ, разработка происходит не на уровне команд для процессора, а на

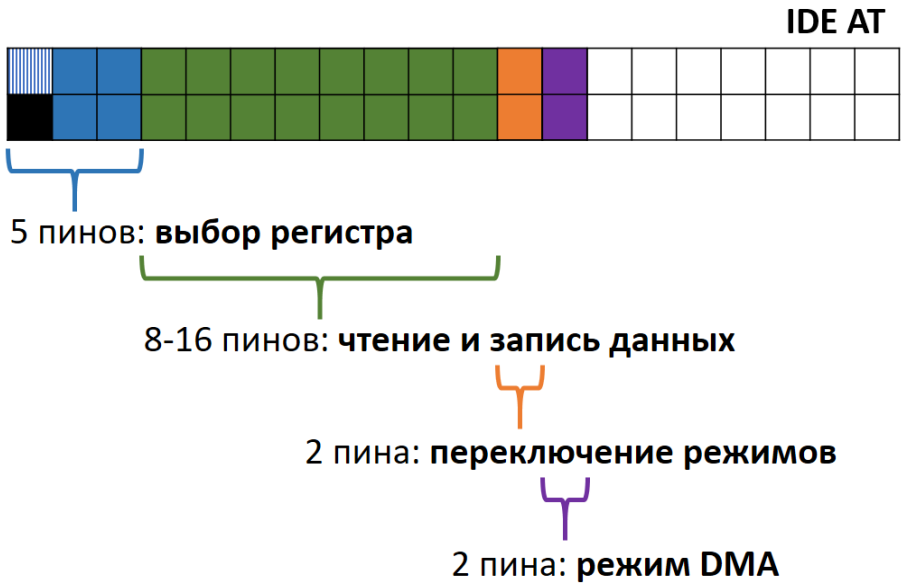

Рис 2. Требуемые пины для взаимодействия с интерфейсом IDE AT

уровне логических функций, что позволяет создать требуемую аппаратную цифровую схему. Полезная нагрузка такой схемы будет многократно выше эффективности работы микроконтроллера, где процессор выполняет множество операций, требуемых ему для работы с предзагруженным кодом. Таким образом, ППВМ позволяет в разы увеличить скорость работы с НЖМД, что увеличит скорость копирования информации.

Помимо этого, блочное устройство ППВМ позволяет производить параллельные вычисления, что дает возможность обрабатывать информацию во время ее копирования, осуществляя вычисление хеш-суммы, и не оказывать влияния на скорость копирования данных.

Разработка прототипа на ППВМ значительно упрощает переход на микросхемы ASIC. Ввиду их схожего строения переход от программируемой модели к производству аппаратных элементов происходит с меньшими временными затратами. Разработка под ППВМ является предпоследним этапом перед получением конечного устройства дубликатора данных, который будет работать на максимально возможных скоростях.

Несмотря на высокую скорость работы микросхемы ППВМ, работа с жестким диском в режиме PIO не позволит развить целевую скорость передачи данных. Для осуществления работы с НЖМД в режиме DMA при разработке дубликатора данных на ППВМ возникает задача реализации DMA контроллера, который должен обладать следующими функциями: определение адреса в буферной памяти, увеличение счетчика адреса, изменение состояния регистра занятости DMA контроллера.

В результате проведенных исследований установлено, что использование контролера Teensy 3.6 возможно только через интерфейс IDE, что не позволяет обеспечить высокую производительность дублирования данных при проведении КТЭ. Напротив, реализация экспериментальной модели дубликатора с интерфейсом SATA на базе ППВМ позволяет достичь максимальных скоростей передачи данных, не влияя на их целостность, что дает возможность перехода к следующей стадии разработки устройства.

Литература

1. ACPO Good Practice Guide for Digital Evidence, Version 5 (October 2011) URL: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (дата обращения: 31.01.2019)

2. Суханов М. О тестировании загрузочных носителей (Live CD, Live USB) с операционными системами на основе Linux, используемых в судебно-экспертной деятельности. URL: http://www.computer-forensics-lab.org/lib/Библиотека/Аналитические_статьи/190/ (дата обращения: 31.01.2019)

3. Graeme B. Bell, Richard Boddington. Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? // Journal of Digital Forensics, Security and Law: Vol. 5 : No. 3 , Article 1. / 2010.

4. Зулькарнеев И.Р., Карпов М.Г., Нестор В.О., Семенов Д.Ю. Концепция создания криминалистического дубликатора данных. // Вестник УрФО № 1(27) / 2018, с. 42–46.

5. Зулькарнеев И.Р., Карпов М.Г., Семенов Д.Ю. Анализ проблем реализации устройств с использованием низкобюджетных плат для целей компьютерной криминалистики. // Математическое и информационное моделирование. Сборник научных трудов (16) / 2018, с. 117-121.

6. ATA Interface Reference Manual // Seagate. URL: ftp://ftp.seagate.com/acrobat/reference/111-1c.pdf (дата обращения: 19.09.2018)

7. Serial ATA Revision 3.0 // Serial ATA International Organization. URL: http://www.lttconn.com/res/lttconn/pdres/201005/20100521170123066.pdf (дата обращения: 19.09.2018)

8. Зотов Валерий Особенности архитектуры нового поколения ПЛИС FPGA фирмы xilinx серии Spartan-6 // Компоненты и Технологии. 2009. №98. URL: https://cyberleninka.ru/article/n/osobennosti-arhitektury-novogo-pokoleniya-plis-fpga-firmy-xilinx-serii-spartan-6 (дата обращения: 31.01.2019).

9. Asano S., Maruyama T. and Yamaguchi Y. Performance comparison of fpga, gpu and cpu in image processing // in International Conference on Field Programmable Logic and Applications, 2009. FPL 2009, 2009. - P. 126-131.

References

1. ACPO Good Practice Guide for Digital Evidence, Version 5 (October 2011) URL: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (дата обращения: 31.01.2019)

2. Suhanov M. O Tests of Boot media drive (Live CD, Live USB) with linux based operating system, used in forensic activities. URL: http://www.computer-forensics-lab.org/lib/Библиотека/Аналитические_статьи/190/ (дата обращения: 31.01.2019)

3. Graeme B. Bell, Richard Boddington. Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? // Journal of Digital Forensics, Security and Law: Vol. 5 : No. 3 , Article 1. / 2010.

4. Zulkarneev I.R., Karpov M.G., Nestor V.O., Semenov D.Y. The concept of criminalistic data duplicarot developing // Vestnik URFO. Cyber space security № 1(27) / 2018, с. 42–46.

5. Zulkarneev I.R., Karpov M.G., Semenov D.Y. Analysis the problems of devices implementation using low-budget boards for computer forensics // Mathematical and information modeling — 2018. — С. 117-121

6. ATA Interface Reference Manual // Seagate. URL: ftp://ftp.seagate.com/acrobat/reference/111-1c.pdf (дата обращения: 19.09.2018)

7. Serial ATA Revision 3.0 // Serial ATA International Organization. URL: http://www.lttconn.com/res/lttconn/pdres/201005/20100521170123066.pdf (дата обращения: 19.09.2018)

8. Zotov V. Architecture features of the new generation Xilinx's Spartan-6 series PLD FPGA // Components and technologies. 2009. №98. URL: https://cyberleninka.ru/article/n/osobennosti-arhitektury-novogo-pokoleniya-plis-fpga-firmy-xilinx-serii-spartan-6 (дата обращения: 31.01.2019).

9. Asano S., Maruyama T. and Yamaguchi Y. Performance comparison of fpga, gpu and cpu in image processing // in International Conference on Field Programmable Logic and Applications, 2009. FPL 2009, 2009. - P. 126-131.

ЗУЛЬКАРНЕЕВ Искандер Рашитович, старший преподаватель, кафедра информационной безопасности, Тюменский государственный университет. 25003, г. Тюмень, ул. Володарского, д. 6. E-mail: i.r.zulkarneev@utmn.ru

КАРПОВ Михаил Георгиевич, студент, кафедра информационной безопасности, Тюменский государственный университет. 25003, г. Тюмень ул. Володарского, д. 6. E-mail: m.g.karpov@utmn.ru

НЕСТОР Владимир Олегович, студент, кафедра информационной безопасности, Тюменский государственный университет. 25003, г. Тюмень ул. Володарского, д. 6. E-mail v.o.nestor@utmn.ru

ZULKARNEEV Iskander, Senior Lecturer, Information Security Department, Institute of Mathematics and Computer Science, University of Tyumen. 6 Volodarskogo St., 625003 Tyumen, Russia. E-mail: i.r.zulkarneev@utmn.ru

KARPOV Mikhail, student, Information Security Department, Institute of Mathematics and Computer Science, University of Tyumen. 6 Volodarskogo St., 625003 Tyumen, Russia. E-mail: m.g.karpov@utmn.ru

NESTOR Vladimir, student, Information Security Department, Institute of Mathematics and Computer Science, University of Tyumen. 6 Volodarskogo St., 625003 Tyumen, Russia. E-mail: v.o.nestor@utmn.ru