УДК 004.056.5 Вестник УрФО № 1(35) / 2020, с. 5–11

Субботин С. Д., Поршнев С. В., Пономарева О. А. DOI: 10.14529/secur200101

ИССЛЕДОВАНИЕ ПОВЕДЕНИЯ ИНФОРМАТИВНЫХ СИГНАЛОВ ОТ НАКОПИТЕЛЯ НА ЖЕСТКИХ МАГНИТНЫХ ДИСКАХ ПРИ ОБРАБОТКЕ ИНФОРМАЦИИ В РАЗНЫХ ОБЛАСТЯХ ДИСКА

В статье демонстрируется изменение спектра информативных сигналов во время моделирования работы (чтения или записи информации) накопителя на жестких магнитных дисках в разных его областях с помощью специализированного программного обеспечения из состава программно-аппаратных комплексов для проведения инженерных исследований и исследований на сверхнормативные побочные электромагнитные излучения и наводки с целью обнаружения возможных частот информативных сигналов (по которым вероятна утечка обрабатываемой информации в том числе ограниченного распространения).

Ключевые слова: *специальные исследования, СИ, накопитель на жестких магнитных дисках, НЖМД, информативные сигналы, электрические сигналы, ПЭМИН, тест-программа, электромагнитное излучение, ЭМИ, защита информации, канал утечки информации, интерфейс SATA.*

THE STUDY OF THE BEHAVIOR OF INFORMATIVE SIGNALS FROM THE ON HARD DISK DRIVE WITH THE PROCESSING OF INFORMATION IN DIFFERENT AREAS OF THE DISK

The article demonstrates the change in the spectrum of informative signals during the simulation of work (reading or writing information) hard disk drive in its different areas with the help of specialized software from the composition of software and hardware complexes for engineering research and research transient electromagnetic pulse emanation standard in order to detect the possible frequencies of informative signals (which are likely to leak the processed information including of limited distribution).

Keywords: *special study, hard disk drive, HDD, informative signals, electrical signal, TEMPEST, test program, electromagnetic radiation, EM radiation, information protection, information leakage channel, SATA interface.*

Одним из важных элементов основных технических средств и систем (далее – ОТСС) является накопитель на жестких магнитных дисках (далее – НЖМД), которым не стоит пренебрегать при проведении специальных исследований (далее – СИ). Классический IDE интерфейс НЖМД – параллельный, а интерфейсы с параллельным кодированием и разрядностью выше 16 как опасные по каналу ПЭМИН уже рассматривать не имеет смысла, также вид данного интерфейса все реже используется, а вот интерфейс SATA в различных своих вариантах является последовательным. Информативные сигналы от SATA интерфейса выявляются по-разному, часто их за пределами корпуса системного блока обнаружить просто не удается [1]. Но это не означает, что если специалисту не удалось их обнаружить, то их нет вообще, ведь если сегодня существующими техническими средствами потенциальный противник не смог осуществить разведку, цель которой определить – что передавалось в конкретный момент времени, ноль или единица, завтра усовершенствовав свои навыки и средства разведки он сможет реализовать съем необходимой информации.

Цель статьи установить изменение спектра информативных сигналов во время моделирования работы НЖМД в разных его областях тест-сигналами, создаваемыми специализированным программным обеспечением (далее – тест-программы) из состава комплексов для проведения инженерных исследований и исследований на сверхнормативные побочные электромагнитные излучения и наводки в конкретной модели НЖМД, представленой в табл. 1 и 3 [2].

Детальные характеристики исследуемого НЖМД из официальной документации представлены в табл. 2 и 3 [3].

Поиск информативных сигналов от исследуемого НЖМД осуществлялся техническими средствами, представленными в табл. 3.

В качестве тест-сигналов использовались тест-программы: «макет специального теста дисковых накопителей» и «СИГУРД-Test» с настроенным сплошным спектром тест-сигнала и параметром заполнения двоичным кодом «1010101» для режимов чтения и записи (см. рис. 1).

Перед проведением СИ исследуемый

Таблица 1

Данные об объекте исследования

Наименование исследуемого устройства	Марка, модель	Серийный номер	Интерфейс
НЖМД	Seagate Barracuda 7200.10 ST3250410AS (250 Gb)	9RY0B525	SATA 2

Таблица 2

Подробные характеристики Seagate Barracuda 7200.10

Количество дисков	1
Количество считывающих головок	2
Гарантированное количество секторов	488 397 168
Количество секторов на дорожке	63
Количество дорожек на всем диске	488 397 168 / 63 = 7 752 336
Количество цилиндров	7 752 336 / 2 = 3 876 168
Скорость вращения шпинделя	7200 об/мин

Таблица 3

Технические средства для проведения исследования

Наименование средств и программ для измерений	Тип	Заявленный производителем диапазон частот, МГц	Фактически использованный диапазон частот, МГц
Программно определяемая радиосистема (SDR)	USRP B210	70 - 6000	34,5 - 6001 (расширен программой USRP Spectrum Scanner)
Антенна широкополосная всенаправленная	Gabil GRA-3000M	2 - 3000	34,5 - 3000
Антенна широкополосная всенаправленная	Ultra-Base Antenna 08-ANT-0861	25 - 6000	3001 - 6000
Программное обеспечение	USRP Spectrum Scanner (FFT)	-	-

НЖМД подвергся полному форматированию в файловой системе NTFS со стандартным размером кластера в 4096 байт. Далее, применив тест-программы, в списке доступных носителей был выбран исследуемый НЖМД. После нажатия кнопки «Запись» отправляется команда считывающим головкам НЖМД на запись тест-файла в ближайшую свободную область диска. Таким образом было записано два тест-файла программой «макет специального теста дисковых накопителей» и два тест-файла программой «СИГУРД-Test» с разными именами. Тест-программы представлены на рис. 1. Затем программой WinHex каждый второй записанный тест-файл был перенесен в другую область диска переназначением кластера для изменения положения считывающих головок НЖМД при обращении к этим файлам.

После проведения СИ ПЭМИН, результат которого приведен в табл. 4 видно, что спектр выявленных информативных сигналов от исследуемого устройства отличается в зависимости от расположения тест-файла на диске (от положения считывающих головок).

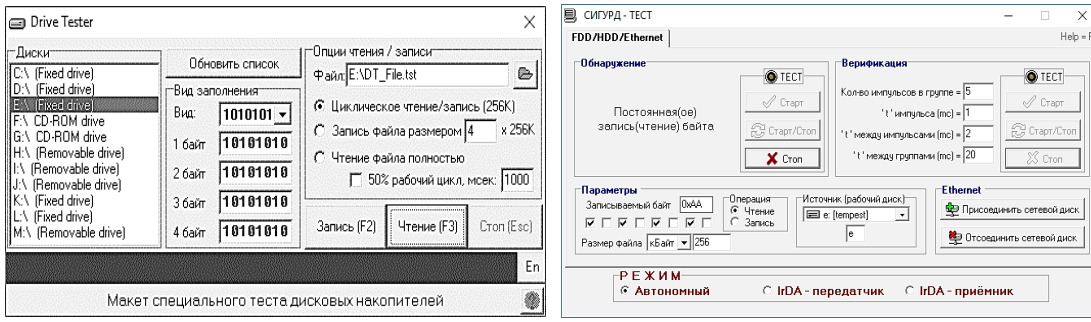

Рис. 1. Интерфейс тест-программ: «Макет специального теста дисковых накопителей» и «СИГУРД-Test»

Таблица 4

Результат исследования НЖМД

№ п/п	Частота информативного сигнала, МГц	Тест режим	Информативный сигнал при тест-файле в первой области НЖМД	Информативный сигнал при тест-файле во второй области НЖМД
1.	247,165	Запись	Присутствует	Присутствует
2.	254,323	Чтение или Запись	Присутствует	Отсутствует
3.	255,255	Чтение	Отсутствует	Присутствует
4.	300,961	Чтение	Присутствует	Присутствует
5.	339,042	Чтение	Присутствует	Присутствует
6.	508,640	Чтение или Запись	Присутствует	Отсутствует
7.	529,836	Чтение или Запись	Присутствует	Отсутствует
8.	1729,422	Запись	Присутствует	Присутствует
9.	1929,700	Запись	Присутствует	Присутствует

Также был зафиксирован электрический сигнал от НЖМД на тактовой частоте 3000,108 МГц интерфейса SATA 2 и частоте 6000,213 МГц, не имеющий признаков информативности от тест-программ, но возникающий при включении исследуемого НЖМД, поэтому данные сигналы во внимание не берутся.

Поиск частот информативных сигналов исследуемого НЖМД осуществлялся в ручном режиме с полосой пропускания измерительного приемника от 1до 10 МГц для диапазона от 34,5 МГц до 3000 МГц и 20 МГц от 3000 МГц до 6000 МГц, рис. 2.

На процесс выявления сигналов ограничений не существует, поэтому антенна размещалась в месте максимального излучения, рис. 3. Поставив разведчика в лучшие условия, но худшие для нас, мы уменьшаем вероятность некачественной защиты обнаруженного информативного сигнала.

Существующие нормативно-методические документы по проведению СИ требуют осуществлять поиск информативных сигналов с разных сторон исследуемого элемента ОТСС, а поскольку сам НЖМД небольшого размера и внутри механические части отвечающие за процесс записи и чтения, являются миниатюрными, то расположение измерительной антенны вряд ли повлияет на результат исследования.

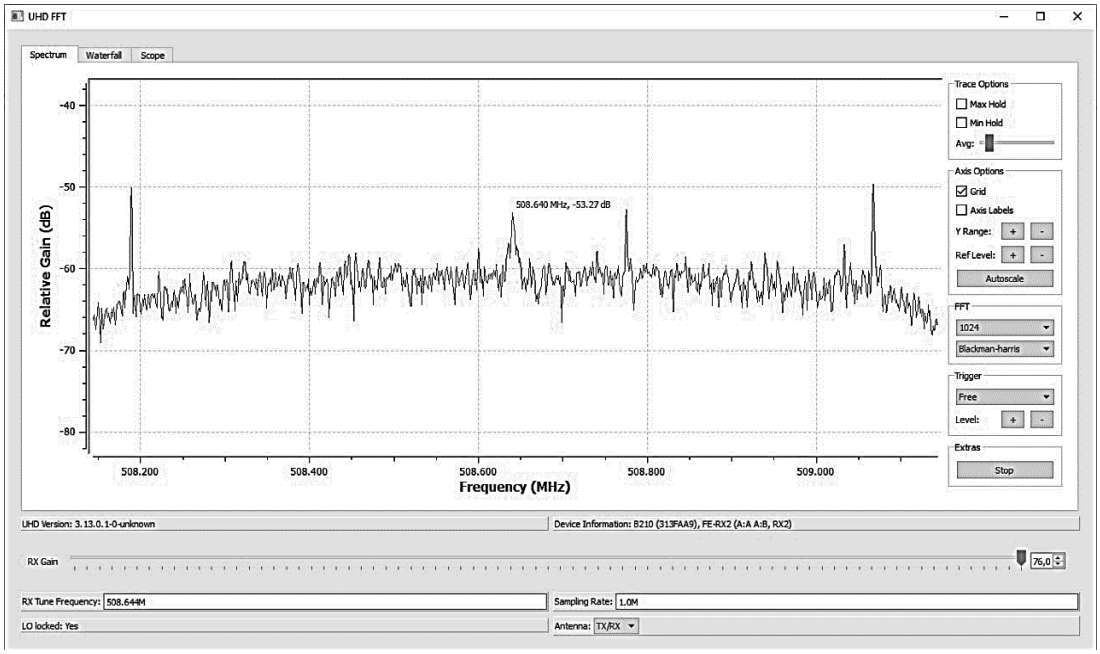

Рис. 2. Интерфейс программы USRP Spectrum Scanner (FFT)

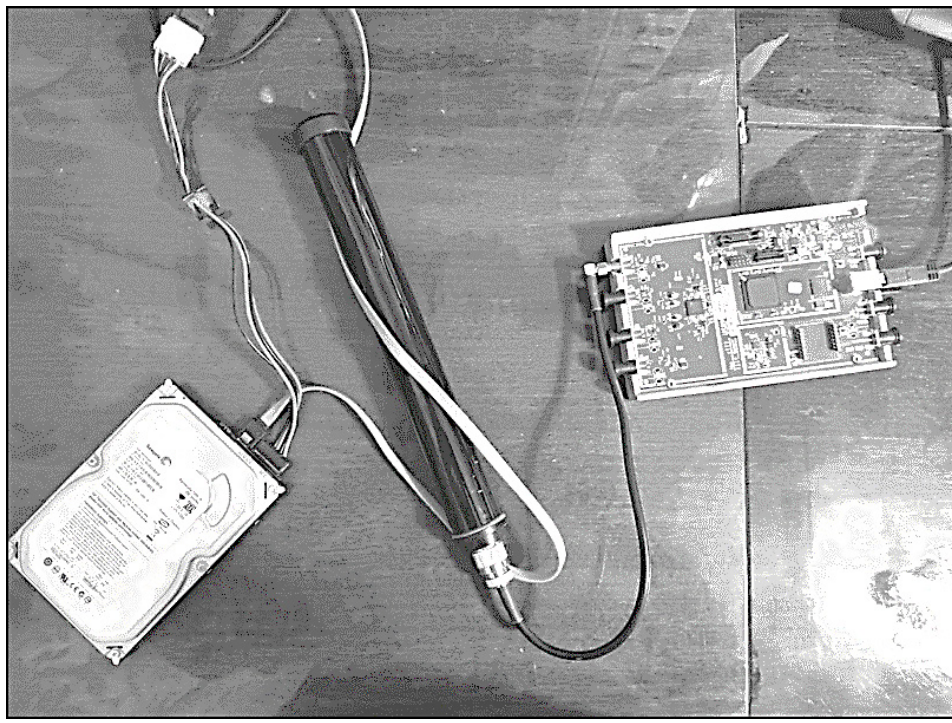

Рис. 3. Проведение поиска информативных сигналов от НЖМД

Рассмотрев принцип работы НЖМД, учитывая, что считывающие головки привязаны к месту обработки информации на диске, можно сделать вывод, что видимое изменение спектра связано с геометрическим положением считывающих головок внутри конструкции НЖМД, а рассмотренные тест-программы, моделирующие работу НЖМД, не учитывают данную особенность. Объяснение изменения спектра сигнала относительно расположения считывающих головок НЖМД при обработке информации заключается в различном переотражении сигнала из-за геометрии самого корпуса НЖМД и его элементов внутри, а также в изменении угловой скорости и длины окружности конкретной дорожки диска.

Почему необходимо проводить СИ НЖМД, моделируя обработку информации в разных областях диска? Потому что файлы со временем имеют свойство фрагментироваться по всей области диска. Либо, когда различные действия пользователя связанные с обработкой информации на компьютере провоцируют появление новых частот информативных сигналов, приводя актуальный протокол технического контроля в несоответствие текущему состоянию системы из-за многократного освобождения или заполнения неопределенного пространства НЖМД за сессию.

Для эффективного проведения СИ НЖМД предлагается разработка тест-программы, с возможностью учёта количества дисков внутри НЖМД, а также положение считывающих головок при обработке информации, позволяя специалисту записывать тест-файл в разные области диска независимо от текущего объема НЖМД.

Литература

1. Кондратьев А.В. Техническая защита информации. Практика работ по оценке основных каналов утечки. – М.: Горячая линия – Телеком, 2016. — 304 с. – ISBN 978-5-9912-0574-0.

2. Субботин С.Д., Поршнев С.В., Пономарева О.А. Исследование эффективности тест-сигналов, создаваемых специализированным программным обеспечением при проведении специальных исследований накопителей на жестких магнитных дисках для выявления технического канала утечки информации ПЭМИН // Сборник трудов XVIII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства». – Магнитогорск : Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2019. – С. 53-58 – ISBN 978-5-9967-1764-4.

3. Product Manual Barracuda 7200.10 Serial ATA. [Электронный ресурс] Seagate.com. URL: https://www.seagate.com/staticfiles/support/disc/manuals/deskt- op/Barracuda%207200.10/100402371k.pdf.

References

1. Kondrat'ev A.V. Tehnicheskaja zashhita informacii. Praktika rabot po ocenke osnovnyh kanalov utechki. [Technical protection of information. Practice of works on estimation of the main channels of leakage]. – M.: Gorjachaja linija – Telekom, 2016. 304 s. – ISBN 978-5-9912-0574-0.

2. Subbotin S.D., Porshnev S.V., Ponomareva O.A. Issledovanie jeffektivnosti test-signalov, sozdavaemyh specializirovannym programmnym obespecheniem pri provedenii special'nyh issledovanij nakopitelej na zhjostkih magnitnyh diskah dlja vyjavlenija tehnicheskogo kanala utechki informacii PJEMIN [Study of the effectiveness of test signals generated by specialized software during special studies of hard disk drives to identify the technical potential of information leakage TEMPEST] // Sbornik trudov XVIII Vseros-siyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh «Bezopasnost' informatsionnogo prostranstva» [Proceedings of the XVIII All-Russian Scientific and Practical Conference of Students, Graduate Students and Young Scientists «Information Space Security»]. Magnitogorsk, Izd-vo Magnitogorsk. gos. tekhn. un-ta im. G.I. Nosova, 2019, pp. 302-306. ISBN 978-5-9967-1764-4.

3. Product Manual Barracuda 7200.10 Serial ATA. [Электронный ресурс] Seagate.com. URL: https://www.seagate.com/staticfiles/support/disc/manuals/deskt- op/Barracuda%207200.10/100402371k.pdf.

СУББОТИН Станислав Дмитриевич, аспирант Института радиоэлектроники и информационных технологий - радиотехнический факультет Уральского федерального университета им. Первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: stwantod@gmail.com.

ПОШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность» Уральского федерального университета им. Первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: s.v.porshnev@urfu.ru.

ПОНОМАРЕВА Ольга Алексеевна, старший преподаватель Института радиоэлектроники и информационных технологий - радиотехнический факультет Уральского федерального университета им. Первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: o.a.ponomareva@urfu.ru.

SUBBOTIN Stanislav Dmitrievich, Postgraduate of Institute of Radio electronics and Information

Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, Mira str., 19. E-mail: stwantod@gmail.com.

POSHNEV Sergej Vladimirovich, Doctor of Technical Sciences, Full Professor, Head of Unit, Training and Research Center «Information Security», Ural Federal University named after first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, Mira str., 19. E-mail: s.v.porshnev@urfu.ru.

PONOMAREVA Olga Alekseevna, Senior Lecturer of Institute of Radio electronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin. 620002, Yekaterinburg, Mira str., 19. E-mail: o.a.ponomareva@urfu.ru.