

ОСОБЕННОСТЬ ИЗМЕРЕНИЯ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ИНТЕРФЕЙСА SATA

Развитие высокоскоростных интерфейсов взаимодействия периферийного оборудования вычислительной техники не только увеличивает пропускную способность, но и увеличивает риск несанкционированного доступа путем перехвата побочных электромагнитных высокочастотных излучений информационных интерфейсов. В настоящее время наиболее распространёнными являются следующие интерфейсы SATA1, SATA2 и SATA 3. В целом, развитие версий SATA и кабелей в значительной степени способствовало развитию возможностей хранения и передачи данных. Излучение кабеля SATA на частоте 1,5 ГГц и выше можно представить как излучение антенны «длинный провод», учитывая длину кабеля от 0.3 до 1 м. С целью повышения селективности излучения от интерфейса SATA в системном блоке компьютера рассматривались две антенны: петлевой вибратор Пистолькорса и круглая рамочная антенна сформированные из кабеля SATA без нарушения его целостности. Проведенные расчеты установили оптимальное значение диаметра круглой рамочной антенны. А исследования спектрального состава электромагнитного излучения интерфейса SATA 1, позволили обнаружить первую гармонику на частоте 1.5 ГГц и последующие вторую, третью и четвертую кратные гармоники. Проведенные исследования показали реальность угрозы утечки информации через побочные электромагнитные излучения интерфейса SATA.

Ключевые слова: побочные электромагнитные излучения, интерфейс, SATA, рамочная антенна, полуволновый вибратор.

Shvyrev B.A., Polikarpov E.S., Anisimov S.L.

THE PECULIARITY OF MEASURING THE SIDE ELECTROMAGNETIC RADIATION OF THE SATA INTERFACE

The development of high-speed interfaces for the interaction of peripheral computer equipment not only increases throughput, but also increases the risk of unauthorized access by intercepting side electromagnetic high-frequency radiation of information interfaces. Currently, the most common interfaces are SATA1, SATA2 and SATA 3. In general, the development of SATA and

cable versions has greatly contributed to the development of data storage and transmission capabilities. The radiation of a SATA cable at a frequency of 1.5 GHz and above can be represented as the radiation of a "long wire" antenna, given the cable length from 0.3 to 1 m. In order to increase the selection of radiation from the SATA interface, two antennas were considered in the computer system unit: a Pistolcors loop vibrator and a round frame antenna formed from a SATA cable without violating its integrity. The calculations carried out have established the optimal value of the diameter of the circular frame antenna. The conducted studies of the spectral composition of the electromagnetic radiation of the SATA 1 interface made it possible to detect the first harmonic at a frequency of 1.5 GHz and the subsequent second, third and fourth multiple harmonics. The conducted research has shown the reality of the threat of information leakage through the side electromagnetic radiation of the SATA interface.

Keywords: side electromagnetic radiation, interface, SATA, frame antenna, half-wave vibrator.

Развитие высокоскоростных интерфейсов взаимодействия периферийного оборудования вычислительной техники не только увеличивает пропускную способность, но и увеличивает риск несанкционированного доступа путем перехвата побочных электромагнитных высокочастотных излучений информационных интерфейсов. Одним из высокоскоростных интерфейсов вычислительной техники является SATA. Данный интерфейс достаточно новый и обладает особенностями. В открытых источниках вопросы исследования побочных электромагнитных излучений интерфейсов накопителей на жестких дисках представлены в источнике [1]. Анализ исследований скрытых технических каналов утечки информации рассматривается в источнике [2], анализ терминологии в источнике [3]. Утечка информации по техническим каналам за счет побочных электромагнитных излучений интерфейсов передачи данных обсуждается в источниках [3, 4], методы радиомониторинга в источнике [5].

Обнаружение и исследование излучения

от достаточно нового высокоскоростного интерфейса SATA является актуальной задачей.

SATA — это командно-транспортный протокол, который определяет способ передачи данных между материнской платой компьютера и устройствами массового хранения, такими как жесткие магнитные диски (HDD), оптические приводы и твердотельные накопители (SSD). Как следует из названия, SATA основан на технологии последовательной передачи сигналов, при которой данные передаются в виде последовательности отдельных битов.

Рассматривать классический параллельный IDE интерфейс уже нет смысла. Во-первых, параллельный (следовательно, менее «опасный»), во-вторых уже всё реже и реже встречающийся. Его место в дисковых интерфейсах безраздельно занимает интерфейс SATA в различных своих вариантах.

В настоящее время наиболее распространенными являются следующие интерфейсы SATA1, SATA2 и SATA3 с параметрами, приведенными в табл. 1.

Таблица 1

Скорости передачи данных интерфейса SATA

Стандарт	Пропускная способность	Скорость передачи данных
SATA I	1.5 Гбит/сек	150 Мбит/сек
SATA II	3 Гбит/сек	300 Мбит/сек
SATA III	6 Гбит/сек	600 Мбит/сек

Первая версия SATA, представленная в 2003 году, имела пропускную способность 1,5 Гбит/с и скорость передачи данных 150 Мбит/с. В 2004 году был выпущен SATA 2.0 с удвоенной пропускной способностью и скоростью передачи данных, достигнув 3,0 Гбит/с и 300 Мбит/с соответственно. Четыре

года спустя, в 2008 году, был представлен интерфейс SATA 3.0 с еще более высокими характеристиками, обеспечивающий пропускную способность 6,0 Гбит/с и скорость передачи данных 600 Мбит/с. Эти улучшения в технологии SATA позволили ускорить и повысить эффективность передачи данных между

устройствами. В целом, развитие версий SATA и кабелей в значительной степени способствовало развитию возможностей хранения и передачи данных.

Кабели SATA представляют собой 7-кон-

тактный кабель, состоящий из заземления (контакты 1,4,7), передачи (контакты 2,3) и приема (контакты 5,6), изображенный на рис.1.

Дифференциальная пара в кабеле SATA

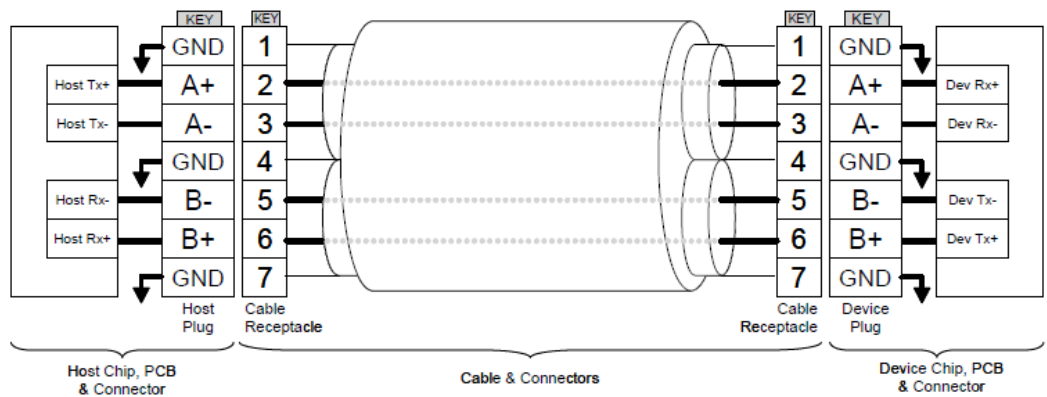


Рис. 1. Схема подключения кабеля / разъема SATA [6].

уменьшает излучающую способность, то есть конструктивно кабель должен меньше излучал побочные электромагнитные излучения.

Из анализа публикаций [7,8,9] следует, что передача данных осуществляется на ча-

стотах СВЧ диапазона начиная с 1,5 ГГц. Для таких высоких частот характерен волновой характер распространения сигнала и кабель SATA можно рассматривать как длинную линию (табл. 2).

Таблица 2

Длина несущей частоты интерфейса SATA

Стандарт	Частота, ГГц	Длина волны, м
SATA I	1,5	0,1998
SATA II	3	0,09993
SATA III	6	0,04996

Наличие дифференциальных пар проводников в кабеле SATA уменьшает побочные электромагнитные излучения, что на ряду с значительным электромагнитным зашумлением от элементов материнской платы компьютера, блока питания и контроллеров затрудняет обнаружение излучения именно кабеля SATA. Излучение кабеля SATA на частоте 1,5 ГГц и выше можно представить как излучение антенны «длинный провод», учитывая длину кабеля от 0.3 до 1 м. Такой тип антенн с увеличением ее длины сжимает диаграмму направленности вдоль проводника. С целью повышения коэффициента направленного действия рассматривались две антенны: петлевой вибратор Пистолькорса и рамочная антенна. Петлевой вибратор Пистолькорса достаточно просто реализуется путем формовки кабеля SATA в размере равном пол длине волны. Параметры петлевого вибратора аналогичны разрезному. Коэффициент

усиления полуволнового вибратора равен 0 дБ, однако диаграмма направленности имеет вид восьмерки, что позволяет излучать электромагнитную волну в более определенном направлении. (Рис.2)

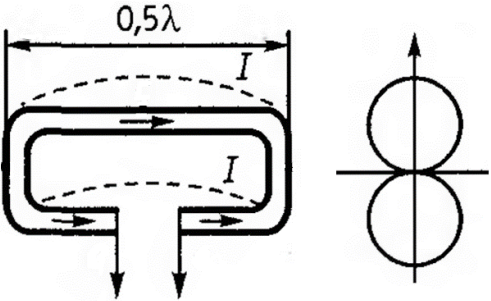


Рис.2. Петлевой вибратор Пистолькорса и его диаграмма направленности [10].

С целью получения большего коэффициента усиления при излучении кабеля SATA без нарушения его целостности построили кру-

глуую рамочную антенну соизмеримую с длиной волны. Рамка создает максимальное излучение с КНД $D_{\max}=1,5$ в своей плоскости и не излучает электромагнитную энергию вдоль оси, и обладает диаграммой направленности в виде восьмерки. Такая антенна обладает кроме селективности по частоте, еще и селективностью по азимуту. Как известно, радиосигнал состоит из электрических и магнитных колебаний. Прием магнитной составляющей радиосигнала обусловлен специальной конструкцией рамочной антенны. Полуволновый диполь, в отличие от рамочной антенны, реагирует на электрическое переменное поле высокочастотного сигнала. У магнитных рамочных антенн есть значительное преимущество они менее чувствительны к бытовым случайным помехам (компьютер, блок питания и т. д.). Другое преимущество магнитной антенны обусловлено её конструкцией: это колебательный контур с довольно высокой добротностью.

Для расчёта воспользовались выражением [10] в полярных координатах рис.3.

$$A_{\varphi\infty}^3 = \frac{2\exp(-ikR)}{4\pi R} \int_0^\pi I_p^3 \cos \phi \exp(jka \sin \theta \cos \phi) d\phi \quad (1)$$
 где a – диаметр рамки, $k = 2\pi/\lambda$, I_p^3 – постоянный ток в рамке

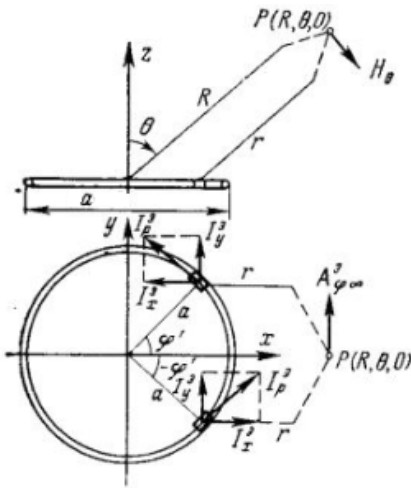


Рис.3. К вычислению поля электрической рамки [4]

Для определения радиуса рамки выражение 1 упростили положив угол $\theta=\pi/2$ и выполнив нормировку на максимальное значением получим

$$D_{\max} = \int_0^\pi \cos \phi \exp(jka \cos \phi) d\phi$$

По результатам численного интегрирования получен график рис.4. Из рис.4 видно, что наибольший КПД рамочной круглой антенны будет при диаметре $a=0.293\lambda$.

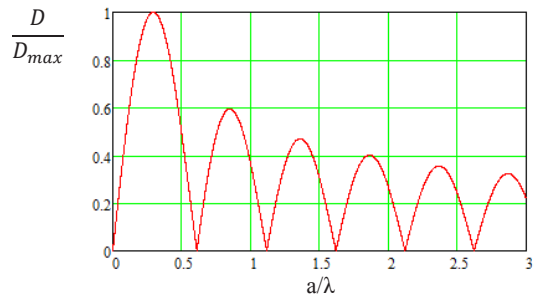


Рис.4. К расчету диаметра рамочной антенны на 6ГГц

Для частоты 1.5 ГГц интерфейса SATA I длина волны 0,1998 м, тогда диаметр антенны будет равен $0.293 \cdot 0.1998 = 0.059$ (м), что соответствует длине окружности немногим меньше длины волны. В зависимости от длинный кабеля SATA удавалось реализовать один или два витка вокруг пластиковой формы соответствующего диаметра.

С целью проверки предложенного способа получения большего коэффициента усиления при излучении кабеля SATA, путем использования рамочной антенны с заданными параметрами, в работе проведены исследования на примере излучения, образующегося при передаче информации на жесткий магнитный диск. Исследование других периферийных устройств подключаемых по SATA I, II, III в работе не приводятся и будут опубликованы позже.

Все последующие измерения проводились с кабелем SATA I, сформированным в одно петлевую круглую рамочную антенну, используемый для подключения накопителя на жестком магнитном диске.

Путем исследования спектрального состава излучаемого электромагнитного поля интерфейса SATA с помощью спектроанализатора, установлено, что интерфейс транслирует электромагнитное излучение в диапазонах с центральными частотами 1,5 ГГц, 3 ГГц, 4,5 ГГц и 6 ГГц.

Порядок проведения измерений ПЭМИ интерфейса SATA:

1. Установить измерительный приемник. Подключить к измерительному приемнику электрическую антенну. Установить требуемые для измерения настройки приемника.
2. Включить СВТ, запустить тестовую программу (тест-сигнал).
3. Перестраивая измерительный приемник в диапазоне частот от 1 ГГц до 9 ГГц произвести поиск сигналов (при необходимости производится смена измерительной антенны).

4. При обнаружении сигнала провести его идентификацию.

Наблюдение за изменением характера и формы сигналов производится визуально на дисплее измерительного приемника.

5. Измерить напряжение сигнала на частоте идентифицированного информативного сигнала при включенном (U_и) и выключенном (U_ш) тесте, дБ (мкВ).

В состав лабораторного стенда, используемого для исследования спектров ПЭМИ накопителя на жёстких магнитных дисках, вхо-

дят: средство вычислительной техники, анализатор спектра R&S FSH13, комплект антенны П6-223, комплект антенны АИР 3-2, сборник тестовых программ «Сигурд-Тест».

Установив необходимые параметры, анализатор спектра выводит ПЭМИ интерфейса SATA на частоте 1,5 ГГц. Пример спектра сигнала представлен на рис. 5.

Далее выключим тестовый режим записи «Сигурд-Тест» и посмотрим, изменится ли спектр. Изменения спектра представлены на рис. 6.

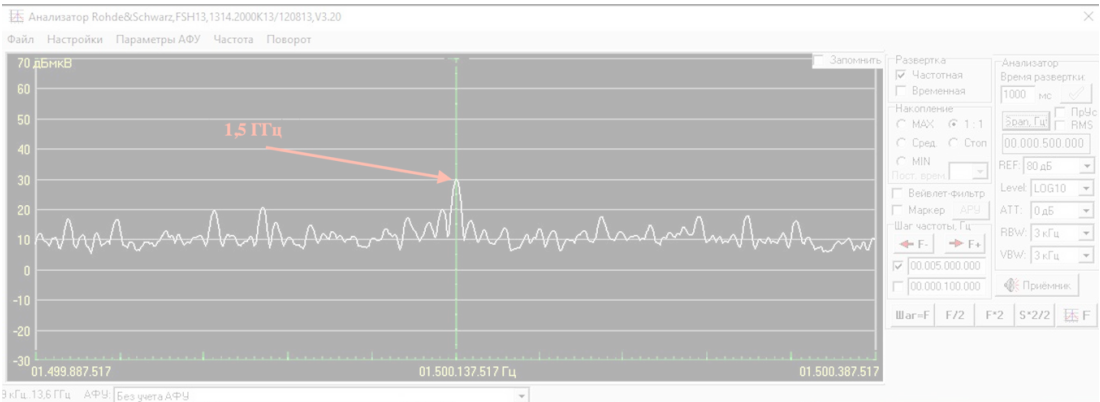


Рис. 5. Спектр сигнала на частоте 1,5 ГГц, SPAN 500 кГц

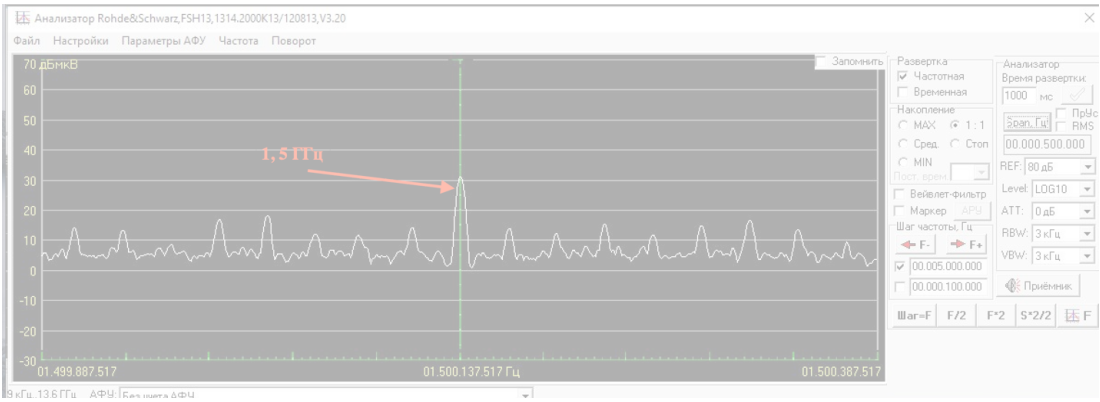


Рис. 6. Спектр сигнала при выключенном режиме записи

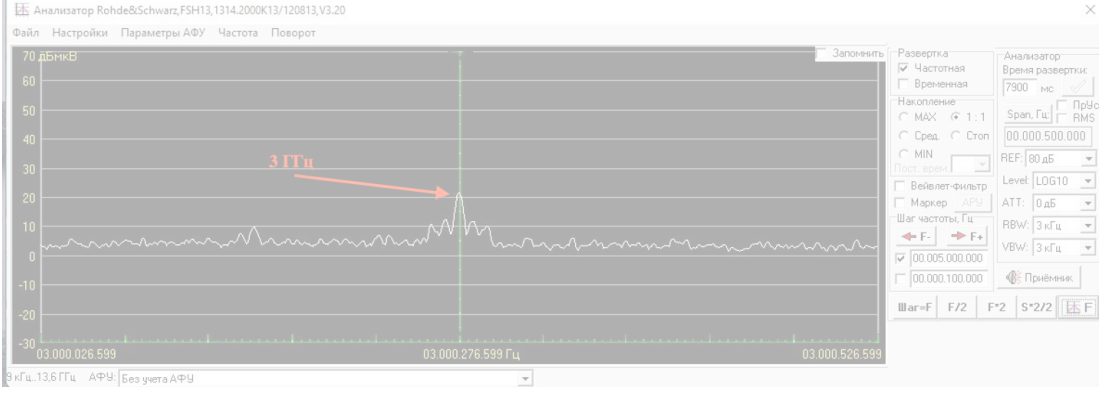


Рис. 7. Вторая гармоника

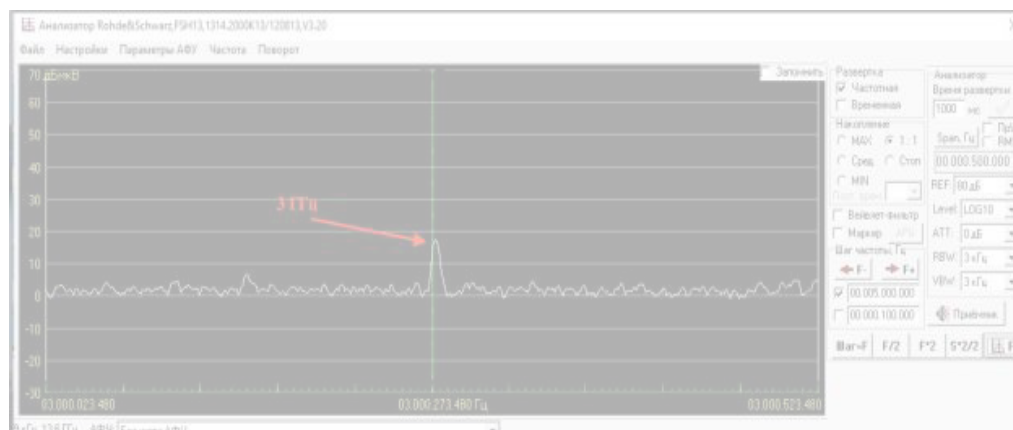


Рис. 8. Спектр сигнала при выключенном режиме

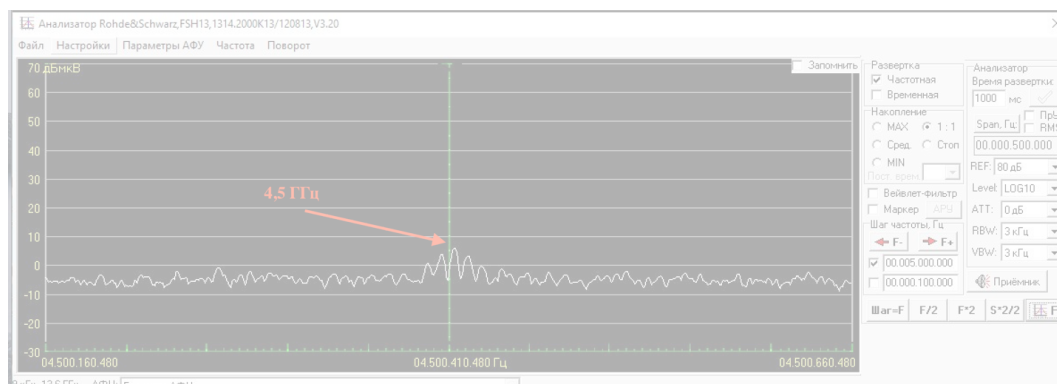


Рис. 9. Третья гармоника

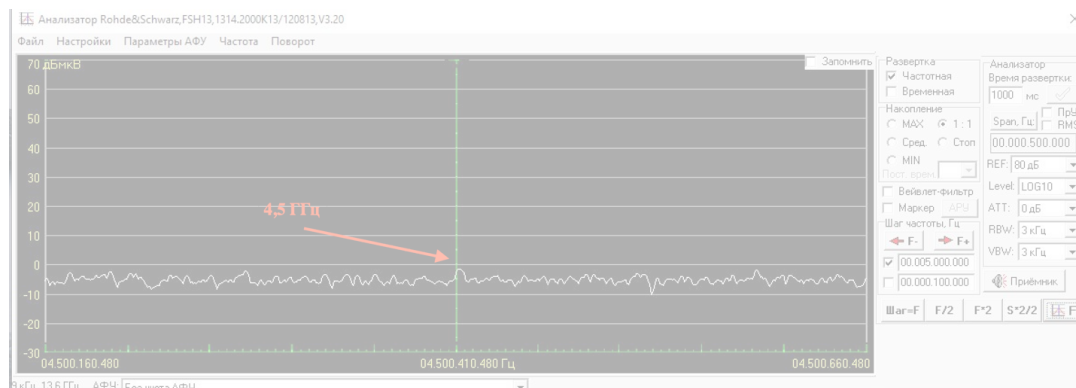


Рис. 10. Спектр сигнала при выключенном режиме



Рис. 11. Четвертая гармоника



Рис. 12. Спектр сигнала при выключенном режиме

Путем сравнения спектрограмм можно заметить, что спектр сигнала при включении/выключении теста действительно изменяется.

Следующая гармоника находится около 3 ГГц, поэтому необходимо включить тестовую программу в режим «Чтения» и выставить центральную частоту 3 ГГц и искать вторую гармонику рядом. Вторая гармоника представлена на рис. 7.

Чтобы убедиться, что это наша вторая гармоника выключаем режим «Чтения». Результат представлен на рис. 8.

Следующая гармоника находится около 4,5 ГГц, поэтому выставляем центральную частоту 4,5 ГГц и ищем сигнал. Третья гармоника представлена на рис. 9.

Чтобы убедиться, что это наша третья гармоника выключаем режим «Чтения». Результат представлен на рис. 10.

Четвертая гармоника, выставляем центральную частоту 6 ГГц и ищем спектр. Четвертая гармоника представлена на рис. 11.

Чтобы убедиться, что это наша четвертая гармоника выключаем режим «Чтения». Результат представлен на рис. 12.

Таким образом можно сделать вывод, что утечка информации через побочные электромагнитные излучения интерфейса SATA является реальной угрозой для безопасности данных, передаваемых периферийными устройства, например, HDD, SSD, DVD-Rom. Для всестороннего исследования рассматриваемого канала утечки актуально продолжить исследование различных модификаций интерфейса SATA в сочетании с разнообразными периферийными устройствами. Для предотвращения утечки необходимо использовать специальные средства измерения и проводить соответствующие мероприятия по защите данных. Важным шагом в этом направлении является проведение измерений побочных электромагнитных излучений средств вычислительной техники, что позволяет выявить уязвимые места и принять меры по их устранению.

Литература

1. Субботин С. Д., Поршнев С. В., Пономарева О. А. Исследование поведения информативных сигналов от накопителя на жестких магнитных дисках при обработке информации в разных областях диска // Вестник УрФО. Безопасность в информационной сфере. – 2020. – №. 1 (35). – С. 5-11.
2. Поршнев С. В., Беляев Д. О. Скрытые технические каналы утечки информации, обрабатываемой средствами вычислительной техники: анализ результатов исследований // Вестник УрФО. Безопасность в информационной сфере. – 2020. – №. 4 (38). – С. 5-21.
3. Поршнев С. В., Беляев Д. О. Скрытые технические каналы утечки информации, обрабатываемой в средствах вычислительной техники: анализ действующей нормативно-методической базы, терминология // Вестник УрФО. Безопасность в информационной сфере. – 2021. – №. 1 (39). – С. 5-13.
4. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. М.: Горячая линия – Телеком, 2005.
5. Рембовский А.М., Ашихмин А.В., Козьмин В.А. Радиомониторинг задачи, методы, средства. М.: Горячая линия – Телеком, 2006.
6. Serial ATA International Organization: Serial ATA Revision 3.1. 18-July-2011 Gold Revision https://sata-io.org/system/files/specifications/SerialATA_Revision_3_1_Gold.pdf

7. Испытательная лаборатория к вопросу оценки ПЭМИН цифровых сигналов. Жёсткие диски (HDD), оптические диски (CD, DVD) Автор: Кондратьев А.В. <https://www.mascom.ru/library/statyi/isyatelnaya-laboratoriya-k-voprosu-otsenki-pemin-tsifrovyykh-signalov-zhyestkie-diski-hdd-optichesk.php>
8. Mordechai Guri. SATAn: Air-Gap Exfiltration Attack via Radio Signals From SATA Cables. <https://doi.org/10.48550/arXiv.2207.07413>
9. HDMI Forum. HDMI Forum. <https://web.archive.org/web/20180222200543/https://www.hdmi.org/learningcenter/faq.aspx#1>
10. Марков Г.Т., Сазонов Д.М. Антенны. – М.: Энергия, 1975. – 528 с.

References

1. Subbotin S. D., Porshnev S. V., Ponomareva O. A. Issledovaniye povedeniya informativnykh signalov ot nakopitelya na zhestkikh magnitnykh diskakh pri obrabotke informatsii v raznykh oblastyakh diska // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2020. – №. 1 (35). – S. 5-11.
2. Porshnev S. V., Belyayev D. O. Skrytyye tekhnicheskiye kanaly utechki informatsii, obrabatyvayemoy sredstvami vychislitel'noy tekhniki: analiz rezul'tatov issledovaniy // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2020. – №. 4 (38). – S. 5-21.
3. Porshnev S. V., Belyayev D. O. Skrytyye tekhnicheskiye kanaly utechki informatsii, obrabatyvayemoy v sredstvakh vychislitel'noy tekhniki: analiz deystvuyushchey normativno-metodicheskoy bazy, terminologiya // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2021. – №. 1 (39). – S. 5-13.
4. Buzov G.A, Kalinin S.V, Kondrat'yev A.V. Zashchita ot utechki informatsii po tekhnicheskim kanalam. M.: Goryachaya liniya –Telekom, 2005.
5. Rembovskiy A.M., Ashikhmin A.V., Koz'min V.A. Radiomonitoring zadachi, metody, sredstva. M.: Goryachaya liniya –Telekom, 2006.
6. Serial ATA International Organization: Serial ATA Revision 3.1. 18-July-2011 Gold Revision https://sata-io.org/system/files/specifications/SerialATA_Revision_3_1_Gold.pdf
7. Ispytatel'naya laboratoriya k voprosu otsenki PEMIN tsifrovyykh signalov. Zhostkiye diski (HDD), opticheskiye diski (CD, DVD) Avtor: Kondrat'yev A.V. <https://www.mascom.ru/library/statyi/isyatelnaya-laboratoriya-k-voprosu-otsenki-pemin-tsifrovyykh-signalov-zhyestkie-diski-hdd-optichesk.php>
8. Mordechai Guri. SATAn: Air-Gap Exfiltration Attack via Radio Signals From SATA Cables. <https://doi.org/10.48550/arXiv.2207.07413>
9. HDMI Forum. HDMI Forum. <https://web.archive.org/web/20180222200543/https://www.hdmi.org/learningcenter/faq.aspx#1>
10. Markov G.T., Sazonov D.M. Antenny. – М.: Energiya, 1975. – 528 s.

ШВЫРЕВ Борис Анатольевич, кандидат физико-математических наук, доцент, доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий. Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет МВД России имени В. Я. Кикотя». 117997, Москва, ул. Академика Волгина, д.12. E-mail: bor2275@yandex.ru

SHVYREV Boris Anatolyevich, Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Department of Special Information Technologies of the educational and scientific complex of information Technologies. Federal State Public Educational Establishment of Higher Education "Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V.Y. Kikot". 117997, Moscow, Akademika Volgina str., 12. E-mail: bor2275@yandex.ru

ПОЛИКАРПОВ Евгений Сергеевич, кандидат технических наук, доцент, начальник кафедры специальных информационных технологий учебно-научного комплекса информационных технологий. Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет МВД России имени В. Я. Кикотя». 117997, Москва, ул. Академика Волгина, д.12. E-mail: binox@mail.ru

POLIKARPOV Evgeny Sergeevich, Candidate of Technical Sciences, Associate Professor, Head of the Department of Special Information Technologies of the educational and scientific complex of

information Technologies. Federal State Public Educational Establishment of Higher Education "Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V.Y. Kikot". 117997, Moscow, Akademika Volgina str., 12. E-mail: binox@mail.ru

АНИСИМОВ Сергей Леонидович, кандидат технических наук, доцент кафедры физики и радиоэлектроники. Федеральное государственное казенное образовательное учреждение высшего образования «Воронежский институт МВД России». 394065, Воронеж, проспект Патриотов, д. 53. E-mail: anisimov12@mail.ru

ANISIMOV Sergey Leonidovich, Candidate of Technical Sciences, Associate Professor of the Department of Physics and Radioelectronics. Federal State-owned educational institution of higher Education "Voronezh Institute of the Ministry of Internal Affairs of Russia". 394065, Voronezh, Patriots Avenue, 53. E-mail: anisimov12@mail.ru