Александр А. Голяков¹, Анатолий П. Дураковский², Егор А. Симахин²

¹Учебный центр безопасности информации «МАСКОМ»,

119421, Москва, ул. Новаторов, д.40 корп.1

e-mail: gaa66@mail.ru, <https://orcid.org/0000-0002-8715-3477>

²Национальный исследовательский ядерный университет «МИФИ»,

115409, г. Москва, Каширское шоссе, 31

e-mail: apdurakovskiy@mephi.ru, <http://orcid.org/0000-0002-8311-7735>

e-mail: dekryt@mail.ru, <https://orcid.org/0000-0003-4019-9694>

ПРИМЕНЕНИЕ ГЕНЕРАТОРА ЗАМЕЩЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ РЕАЛЬНОГО
ЗАТУХАНИЯ ИНФОРМАТИВНЫХ СИГНАЛОВ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ
ИЗЛУЧЕНИЙ

DOI: <http://dx.doi.org/10.26583/bit.2018.2.03>

Аннотация. Наиболее трудоемкими операциями при оценке защищенности информации от ее утечки за счет побочных электромагнитных излучений (ПЭМИ) являются работы, связанные с определением реального затухания излученного информативного сигнала. Большой интерес представляет собой задача автоматизации данного вида измерений. На измерение затухания с помощью существующих автоматизированных комплексов требуется значительное время. Поэтому, как правило, измерения проводятся только на ограниченном количестве частот. Вместе с тем, спектр одиночного информативного импульса имеет лепестковую структуру и в каждом частотном лепестке является сплошным. Соответственно измерение значений затухания напряженности электромагнитного поля на отдельных частотах не отражает полноту характеристики затухания. Если же проводить измерения затухания по всему спектру информативного сигнала в заданном диапазоне частот, то необходимо провести несколько тысяч измерений, что делает такой подход не эффективным с точки зрения временных затрат. Современные специализированные автоматизированные измерительные системы (САИС) контроля защищенности по каналам ПЭМИ имеют режим измерения шума системы активной защиты, который можно использовать для измерения реального затухания. В данной работе описан и экспериментально подтвержден более точный и быстрый способ измерения реального затухания информативного сигнала на примере видеоподсистемы монитора с электронно-лучевой трубкой (ЭЛТ) с использованием САИС «Сигурд» и генератора замещения. Применение генератора замещения в автоматизированных измерениях позволяет существенно сократить временные затраты на проведение специальных исследований (СИ) по контролю защищенности информации от утечки за счет ПЭМИ.

Ключевые слова: генератор замещения, информационная безопасность, побочные электромагнитные излучения, реальное затухание.

Для цитирования. ГОЛЯКОВ, Александр А.; ДУРАКОВСКИЙ, Анатолий П.; СИМАХИН, Егор А.. ПРИМЕНЕНИЕ ГЕНЕРАТОРА ЗАМЕЩЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ РЕАЛЬНОГО ЗАТУХАНИЯ ИНФОРМАТИВНЫХ СИГНАЛОВ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ. Безопасность информационных технологий, [S.l.], п. 2, р. 38-53, 2018. ISSN 2074-7136. Доступно на: <<https://bit.mephi.ru/index.php/bit/article/view/1108>>. Дата доступа: 26 apr. 2018. doi:<http://dx.doi.org/10.26583/bit.2018.2.03>.

Alexander A. Golyakhov¹, Anatoly P. Durakovskiy², Egor A. Simakhin²

¹ Educational center of information security "MASKOM",

119421, Moscow, ul. Novatorov, 40 korp.1

e-mail: gaa66@mail.ru, <https://orcid.org/0000-0002-8715-3477>

²National research nuclear university "MEPHI",

115409, Moscow, Kashirskoye highway, 31

e-mail: apdurakovskiy@mephi.ru, <http://orcid.org/0000-0002-8311-7735>

e-mail: dekryt@mail.ru, <https://orcid.org/0000-0003-4019-9694>

Use of generator substitution to determine the real attenuation of informative signals in the compromising emanation

DOI: <http://dx.doi.org/10.26583/bit.2018.1.03>

Abstract. A determination of real attenuation of information signal's radiation on a way from the source to a possible location of intelligence devices is considered to be the most difficult operation while assessing information security against leakage of electromagnetic emanation. In this context the problem of automation of this kind of measurement is of great interest. It takes considerable effort and time to measure the attenuation by existing automated systems. That is why the measurements are generally taken within the limited range of frequencies only. Along with that, a spectre of a single information impulse has a leaf-structure and is solid on every frequency leaf. So electromagnetic field intensity attenuation measurement carried on the some preselected frequencies is not able to represent the complete attenuation characteristics. The measurements of attenuation in the whole informative signal spectre within the given frequency range requires a few thousand measurements, which makes the current method ineffective and time consuming. The relevant specialized automatized measurement systems of security verification has active protection system noise measurement mode, which can be used to measure the real attenuation. In this article a rather exact method of real attenuation of informative signal of video subsystem of electron-ray tube monitor measurement is described and confirmed in experiment. The measurements were made using specialized automatized system "Sigurd" and video subsystem informative signal noise generator. The described method allows a significant reduction of the time needed for specialized investigations of security verification on electromagnetic emanation.

Keywords: noise generator, information security, compromising emanation, attenuation of electromagnetic field, TEMPEST.

For citation. GOLYAKHOV, Alexander A.; DURAKOVSKIY, Anatoly P.; SIMAKHIN, Egor A.. Use of generator substitution to determine the real attenuation of informative signals in the compromising emanation. IT Security (Russia), [S.l.], n. 2, p. 38-53, 2018. ISSN 2074-7136. Available at: <<https://bit.mephi.ru/index.php/bit/article/view/1108>>. Date accessed: 26 apr. 2018. doi:<http://dx.doi.org/10.26583/bit.2018.2.03>.

Введение

В процессе обработки информации средства вычислительной техники излучают информативные электромагнитные волны. При перехвате данного излучения существует возможность восстановления конфиденциальной информации [1]. В связи с этим появляется потенциальная угроза информационной безопасности – утечка информации по каналу побочных электромагнитных излучений и наводок. Рассматриваемый канал работает фактически в реальном масштабе времени, является пассивным, что не дает возможности владельцу информации обнаружить нарушителя. Все это в совокупности говорит о высоком уровне опасности побочных излучений средств вычислительной техники. Поэтому в последние годы данному техническому каналу утечки информации уделяется пристальное внимание.

Впервые, с точки зрения защиты информации, опасность побочного электромагнитного излучения (или, как называют зарубежные исследователи, «компрометирующего электромагнитного излучения») была продемонстрирована в марте 1985 года на международном конгрессе по защите информации Securecom-85 в Каннах. Голландский инженер Вим ван Эйк, используя устройство в виде доработанного телевизионного приемника, продемонстрировал перехват информации с монитора компьютера, который находился рядом в здании [2]. В 2003 году были проведены эксперименты по исследованию характера и свойств компрометирующих излучений для мониторов с электронно-лучевой трубкой и жидкокристаллических мониторов [3]. В 2010

году группой французских исследователей была показана возможность снятия компрометирующего излучения работы компьютера с линий электропитания, расположенных в доме [4]. В 2011 году авторы [5] проанализировали и провели измерения ПЭМИ клавиатуры с интерфейсом PS/2. Эксперименты, проведенные исследователями, показали, что характеристика сигналов нажатия клавиш может быть восстановлена путем анализа полученных электромагнитных сигналов во временной области, что приводит к компрометации ввода информации с помощью клавиатуры. В 2012 году те же специалисты, проанализировав компрометирующие электромагнитные излучения цифровых сигналов, построили модель компрометирующего излучения [1]. В 2013, в журнале «IEEE Transaction on electromagnetic compatibility» была опубликована статья [6], в которой говорится о сложностях распознавания компрометирующих сигналов LVDS интерфейса мониторов. В 2014 году одной из тем 23-ей международной научно-технической конференции была работа [7], в которой исследуется опасность побочного излучения принтера. В том же году было проведено исследование ПЭМИ интерфейса USB 2.0 при передаче данных [8]. В 2016 году на симпозиуме PIERS, проходившем в Шанхае, была представлена работа польских исследователей [9], в которой описывается исследование компрометирующего излучения VGA и DVI интерфейсов. В том же году на 13-ой международной научно-технической конференции «Actual Problems of Electronics Instrument Engineering (APEIE)», обсуждалась работа отечественных исследователей на тему особенностей идентификации и анализа ПЭМИ от USB-флэш-накопителей [10]. Активно ведутся работы по исследованию компрометирующего излучения смартфонов и их интерфейсов [11-12]. Разрабатываются методы обнаружения и восстановления компрометирующего излучения USB клавиатуры [13-14]. Продолжается работа по разработке программно-аппаратных комплексов поиска компрометирующих излучений [15]. Обширные исследования в этой области показывают на актуальность защиты информации от ее утечки по данному техническому каналу. Особый интерес со стороны специалистов по технической защите информации представляют работы, связанные с определением реального затухания информативных сигналов, позволяющие оценить уязвимость объекта информатизации.

Описание метода определения реального затухания

Измерение реального затухания при проведении СИ по контролю защищенности осуществляют с помощью различных САИС, принцип работы которых основан на передаче по радиоканалу с управляющего компьютера значения частоты, на которой необходимо измерить затухание, на генератор синусоидальных сигналов с передающей антенной, и последующему измерению уровней сигналов, излученных генератором в первой (ближней) и во второй (дальней) точках, параллельно или последовательно в автоматическом или ручном режимах.

Данный подход имеет ряд достоинств и недостатков. К достоинствам можно отнести то, что с использованием генератора синусоидальных сигналов можно проводить измерение затухания на значительных расстояниях. К недостаткам – большие временные затраты на проведение измерений при определении затухания.

Имеющиеся недостатки возможно преодолеть, используя САИС «Сигурд» и мощный, стабильный по времени источник шумового сигнала в заданном диапазоне частот - генератор замещения. В этом случае отпадает необходимость в перестройке генератора синусоидальных сигналов по частоте, что, соответственно, исключает потери времени на установление связи и коммутацию. С учетом быстрогодействия современных анализаторов спектра последовательный анализ существующего диапазона измерений с учетом 20 накоплений можно провести примерно за 5-7 минут.

Для расчета коэффициента затухания информативного сигнала в каждом частотном лепестке целесообразно использовать формулу:

$$K_{отсс(сз)} = \frac{\sqrt{\sum_{j=1}^k (10^{\frac{E_{1j}}{20}})^2}}{\sqrt{\sum_{j=1}^k (10^{\frac{E_{2j}}{20}})^2}}, \quad (1)$$

где $E_{1(2)}$ – напряженность электрической составляющей электромагнитного поля шума генератора замещения при измерении в ближней (дальней) точке от исследуемого технического средства или средства активной защиты (САЗ), дБ(мкВ/м);

k – количество фильтров, укладываемых в одном частотном лепестке.

Однако спектральная плотность информативного сигнала (идеального прямоугольного импульса) распределена по частотному лепестку не равномерно, а имеет форму огибающей $\sin(x)/x$. На рисунке 1 красным цветом представлен его спектр по модулю.

Рис. 1. Спектр информативного сигнала в токопроводящей цепи
(Fig. 1. Spectrum of informative signal)

В силу того, что электромагнитное поле возникает только при изменении напряжения или тока, случайная антенна будет излучать информативный импульс только на фронтах. Таким образом, форма информативного сигнала претерпевает определенные изменения, и спектр излученного сигнала, сохранив размер частотных лепестков, изменит форму. Модуль огибающей спектра сигнала, излученного случайной антенной, показан на рисунке 1 синей линией. Частотный лепесток становится симметричным, максимальная спектральная плотность находится в центре.

В общем случае форма огибающей спектра излученного сигнала зависит от многих факторов, и прежде всего, от формы информативного импульса, длительности фронта и спада, а также от излучательной способности случайной антенны.

Огибающую спектра излученного сигнала в первом приближении для инженерного расчета можно описать функцией:

$$q(f) = \left| \sin\left(\frac{\pi \cdot f}{\Delta F_{\text{л}}}\right) \right|, \quad (2)$$

или

$$q(f) = \left| \sin(\pi \cdot f \cdot \tau_u) \right|, \quad (3)$$

где: f – частота, МГц;

$\Delta F_{\text{л}}$ – ширина частотного лепестка, МГц;

τ_u – длительность импульса, мкс.

Перейдем от огибающей спектра напряженности к огибающей энергетического спектра:

$$q_1(f) = 0,027 \cdot \left(\left| \sin\left(\frac{\pi \cdot f}{\Delta F_{\text{л}}}\right) \right| \right)^2, \quad (4)$$

где 0,027 – нормировочный коэффициент, такой что:

$$\int_0^{\Delta F_{\text{л}}} q_1(f) df = 1. \quad (5)$$

Коэффициент приведен для ширины лепестка 75 МГц.

Для того, чтобы учесть распределение напряженности поля по частотному лепестку целесообразно использовать следующую формулу:

$$K_{\text{OTCC(САЗ)}} = 20 \cdot \lg \left(\left(\sum_{j=1}^k \frac{(10^{E_{2j}/20})^2 \cdot q_1(f_j) \cdot \Delta f_{\phi}}{(10^{E_{1j}/20})^2} \right)^{-1} \right), \quad (6)$$

где $E_{1(2)}$ – напряженность электрической составляющей электромагнитного поля шума генератора замещения при измерении в ближней (дальней) точке от ОТСС (САЗ), дБ(мкВ/м);

k – количество фильтров, укладываемых в одном частотном лепестке;

Δf_{ϕ} – полоса фильтра, которым проводилось измерение, МГц,

Методику определения затухания с учетом формы, огибающей спектра информативного сигнала можно описать следующим образом:

1) Определить форму информативного сигнала с использованием осциллографа или исходя из описания работы интерфейса, описать сигнал функцией от времени $y(t) = f(t)$;

2) Взять производную от функции времени $y_1(t) = \frac{dy(t)}{dt}$;

3) Выполнить преобразование Фурье от функции $y_1(t)$. При достаточно мощном излучении тестового сигнала, определится с формой, огибающей спектра можно задать тест пиксель через 10-20 пикселей, как показано на рисунке 2;

Рис. 2. Форма огибающей спектра частотного лепестка
(Fig. 2. The form of frequency lobe)

- 4) Аппроксимировать огибающую спектра любым известным способом и получить функцию $q(f)$;
- 5) Найти огибающую энергетического спектра $q_1(f)$, провести нормировку;
- 6) Измерить напряженность поля генератора замещения в первой и во второй точках фильтр к фильтру в частотном лепестке;
- 7) Произвести расчет затухания в частотном лепестке с учетом формы, огибающей спектра в соответствии с формулой (6).

Проведение измерений с использованием САИС «Сигурд»

В качестве исследуемого элемента средства вычислительной техники (СВТ) был выбран монитор с электронно-лучевой трубкой. В качестве генератора замещения использовалась совокупность генераторов шума (ГШ) – Соната Р2, ЛГШ-501 и SEL SP-21. Измерения затухания производились на расстоянии 10 м от ЭВМ. Исходными данными для проведения измерений являются значения сигналов и шумов, на найденных частотах гармоник тестового сигнала.

Методику проведения измерения затухания информативных сигналов с использованием САИС «Сигурд» и генератора замещения можно представить следующим образом:

- 1) Используя задание с результатами измерений сигналов и шумов на частотах гармоник тестового сигнала, или создав новое задание, перейти во вкладку «Верификация и измерение» для настройки параметров анализатора спектра при измерении САЗ. Для повышения точности измерений количество накоплений следует выбирать в диапазоне от 15 до 20. Для учета изменений настроек программой нажать кнопку «Сохранить задание», а затем для продолжения работы кнопку «Выбрать текущее задание», как показано на рисунке 3;

Рис. 3. «Параметры заданий» вкладка «Верификация и измерение»
(Fig. 3. "Job options" tab "Verification and measurement")

2) В поле «Выполняемые операции» окна «Задание» перейти во вкладку «САЗ». Заполнить поля «Длительность импульса» и «Порог отсеивания». Расчет длительности импульса может производиться автоматически исходя из значения частоты первой гармоники тестового сигнала, установленной во вкладке «Экспресс-поиск», при нажатии на кнопку «= полупериод $F_{\text{такт}}$ ». Значение порога отсеивания показывает, насколько напряженность поля сосредоточенного источника должна превосходить средний уровень шума САЗ, чтобы не восприниматься за шум. Иллюстрация к данному пункту представлена на рисунке 4;

3) Выставить ГШ в месте размещения СВТ, включить их. Выставить приемную антенну на высоте 1 метр над уровнем поверхности в точке возможного размещения средства разведки в направлении ГШ. Выполнить измерения шума генераторов в дальней точке, нажав кнопку «Старт задания». Выключить ГШ. Поставить галочку в графе «Измерение САЗ в точке 2» и выполнить измерение объектового шума в дальней точке.

4) По окончании работы программы, убедиться в том, что уровень шума от генератора не менее чем на 3 дБ превышает уровень объектового шума, просмотрев полученные измерения. Для этого в окне «Задание» нажать кнопку «Просмотр измерения САЗ». При отрицательном результате следует либо заменить используемые ГШ более мощными, либо произвести измерения на максимально возможном расстоянии, на котором выполняется вышеописанное условие. Для окончания просмотра снятых измерений нажать кнопку «Конец просмотра САЗ». Иллюстрации к данному пункту представлены на рисунках 5а и 5б;

Рис. 4. Вкладка «СА3»
 (Fig. 4. Tab “APS”)

Рис. 5а. Подготовка к просмотру измерений шума
 (Fig. 5a. Preparing to view noise measurements)

Рис. 5б. Просмотр измерений шума
(Fig. 5b. Viewing noise measurements)

5) При положительном результате для проверки расчета затухания, выполняемого системой «Сигурд» по формуле (1), нажать кнопку «Экспорт» для сохранения полученных данных в отдельный текстовый файл с помощью стандартных средств операционной системы управляющей ЭВМ;

6) Включить ГШ. Для корректного учета программой «Сигурд-Дельта» измерений необходимо повторно измерить уровень шума САЗ в дальней точке, нажав кнопку «Старт задания».

7) Выставить приемную антенну на высоте 1 метр над уровнем поверхности и на расстоянии 1 метра от антенны ГШ по оси, соединяющей текущее положение антенны и точку возможного размещения средства разведки. Снять галочку в графе «Измерение САЗ в точке 2» и нажать кнопку «Старт задания»;

8) Для проверки расчета затухания, выполняемого системой «Сигурд» по формуле (1), нажать кнопку «Экспорт» для сохранения полученных данных в отдельный текстовый файл;

9) Выключить ГШ;

10) Открыть расчетную программу «Сигурд-Дельта» нажав кнопку «Расчет» на панели управления программы «Сигурд – Интерфейс». Во вкладке «Атрибуты» программы «Сигурд-Дельта» необходимо выбрать вид исследования, в графе «Вид измерений» выбрать «в эфире», описать исследуемое техническое средство и выбрать средство измерения, с помощью которого проводились измерения. Иллюстрация к пункту 10 представлена на рисунке 6.

11) Для того чтобы программа «Сигурд-Дельта» учла снятый шум от генератора необходимо поставить галочку у поля «САЗ» в графе «'Е' – компонента». При этом появятся вкладки: «'Е' - сигналы», «САЗ для 'Е'» и «Затухание 'Е'»;

12) Перейти во вкладку «'Е' - сигналы». Если для измерения затухания использовалось новое задание, то используя кнопку загрузить сохраненные данные сигналов и шумов на частотах гармоник, либо вручную ввести значения сигналов и шумов из сохраненных результатов выполненного задания. Если для измерения затухания использовалось текущее задание, то значения сигналов и шумов отобразятся автоматически. Внести необходимые изменения в поля: «Предусилитель», «Антенна» и «Фидер».

13) Перейти во вкладку «САЗ для 'Е'». Выставить необходимые настройки устройств в полях «Предусилитель», «Антенна» и «Фидер». Если при измерении шума САЗ антенно-фидерный тракт остался таким же, как при измерении сигналов, то поставить галочку в поле «Антенна, предусилитель и фидерный тракт такие же, как у сигналов».

Рис. 6. Вкладка «Атрибуты»
(Fig. 6. Tab “Attribute”)

Чтобы расчетная программа учла измеренный шум САЗ, необходимо в поле «АЧХ САЗ» выбрать графу «Измеренный спектр». В поле «Вариант измерения САЗ» необходимо выбрать графу «ГШ вблизи СВТ». При этом вместо вкладки «Затухание 'Е'» появится вкладка «Затухание ГШ — Е». Иллюстрация к пункту 13 представлена на рисунке 7;

Рис. 7. Вкладка «САЗ для 'Е'»
(Fig. 7. Tab “APS for 'E'”)

14) Перейти во вкладку «Затухание ГШ-Е». Выставить необходимые настройки устройств в полях «АФУ для т.1» и «АФУ для т.2». Если используемые устройства не изменились после измерения сигналов, то поставить галочку в полях «АФУ такие же, как у сигналов» и «АФУ как у сигналов». В раскрывающемся списке внизу вкладки выбрать графу «Измеренный спектр» для учета программой «Сигурд – Дельта» данных шума

генератора в первой и во второй точках. Иллюстрация к пункту 14 представлена на рисунке 8;

Рис. 8. Вкладка «Затухание ГШ-Е»
(Fig. 8. Tab “Attenuation NG-E”)

15) Перейти во вкладку «Параметры» и выставить необходимые настройки, зависящие от тестового сигнала и ГШ, как представлено на рисунке 9;

Рис. 9. Вкладка «Параметры»
(Fig. 9. Tab “Parameters”)

16) Выбрать формат документа, в котором будет представлен расчет. Для этого необходимо в меню «Файл» выбрать пункт «Вывод отчета...». После выбора формата файла отчета нажать кнопку «Вычислить». На экране появится окно с полем «Вывод протоколов». Необходимо оставить галочку только в пункте «САЗ». И нажать кнопку «Да». Иллюстрация к пункту 16 представлена на рисунке 10.

Рис. 10. Получение протокола
 (Fig. 10. Reception of protocol)

Обработка измерений и результаты эксперимента

В «Протоколе инструментальной оценки эффективности САЗ» в таблице «Полный расчет», представлены полученные при измерении значения напряженности поля шума от генераторов шума «Е_{саз}(В)» и «Е_{саз}(L')» в каждом частотном лепестке в ближней и дальней точках соответственно.

Покажем, что САИС «Сигурд» может использоваться для измерения реального затухания сигналов ПЭМИ с генератором замещения. Для этого необходимо рассчитать коэффициенты затухания по формуле (1) и сравнить с отношением «Е_{саз}(В)»/«Е_{саз}(L')». Для учета формы спектра информативного сигнала при определении затухания произвести расчет по формуле (6). Получение исходных данных из текстовых файлов, нормировка функции огибающей энергетического спектра, а также расчеты по формуле (1) и формуле (6) в третьем частотном лепестке представлены на рисунке 11. Построение графиков шума ГШ в первой и во второй точке показано на рисунке 12.

Рис. 11. Работа в Mathcad
 (Fig. 11. Work in Mathcad)

*Рис. 12. График зависимости снятого шума от частоты
 (Fig. 12. Graph of the frequency dependence of the noise)*

Предварительно необходимо оценить эффективность работы генераторов шума, построив графики зависимости шума от частоты в первой и во второй точках. В текстовых файлах, полученных при измерениях САЗ в ближней и дальней точках необходимо заменить символ «,» на символ «.» для правильного учета данных инженерным математическим ПО Mathcad. На рисунке 12 показано, что шум от генераторов до частоты 1 МГц является неэффективным.

При ширине частотного лепестка в 75 МГц значениями затухания информативного сигнала до частоты 1 МГц можно пренебречь, либо оценить затухание на участке до 1 МГц по наименьшей частоте, на которой значение шума в первой точке в заданное количество раз превосходит значение во второй, при этом получится запас по защищенности.

Для более точного расчета затухания информативного сигнала в частотном лепестке можно получить «чистый» шум от генераторов шума. Для этого последовательно произвести измерения объектового шума в точке 1 и точке 2, сохранить результаты в текстовые файлы. В силу специфики программного обеспечения (ПО) САИС «Сигурд» измерение объектового шума в точке 2 необходимо проводить с настройками как в точке 1. Далее произвести расчет «чистого» шума по формуле:

$$E_{ш_j} = 20 \cdot \lg \left(\sqrt{\left(10^{\frac{E_{гш_j}}{20}} \right)^2 - \left(10^{\frac{E_{ош_j}}{20}} \right)^2} \right), \quad (7)$$

где $E_{ш_j}$ – «чистый» шум на j -ой частоте, дБ(мкВ/м);

$E_{гш_j}$ – напряженность электрической составляющей электромагнитного поля шума генератора замещения при измерении в ближней (дальней) точке от ОТСС (САЗ), дБ(мкВ/м);

$E_{ош_j}$ – напряженность электрической составляющей электромагнитного поля объектового шума при измерении в ближней (дальней) точке от ОТСС (САЗ), дБ(мкВ/м);

Результаты эксперимента представлены в таблице 1.

Таблица 1. Результаты эксперимента

№ п/п	Фц инт. МГц	№№ сигн. интерв.	К _С	К _{Ф1}	К' _{Ф1}	К _{Ф6}	К' _{Ф6}	К _{ГСС}
1	37,5000	1, 2	13,34	14,18	13,26	15,90	18,84	19,442
2	112,5000	3, 4	16,71	15,87	15,87	7,65	7,70	19,831
3	187,5000	5, 6	14,10	13,88	13,88	10,03	10,08	9,913
4	262,5000	7, 8	16,36	16,60	16,60	14,85	14,90	17,553
5	337,5000	9, 10	12,65	12,04	12,04	8,31	8,36	6,746
6	412,5000	11, 12	15,24	15,52	15,05	14,99	15,05	19,389
7	487,5000	13	11,29	11,37	11,38	9,83	9,89	17,817
8	562,5000	14	16,07	16,08	16,09	16,71	16,80	18,495
9	712,5000	15	14,62	14,11	14,11	12,33	12,38	20,141
10	787,5000	16, 17	17,04	17,28	17,28	17,21	16,80	12,657
11	862,5000	18, 19	13,72	13,56	13,56	13,39	9,65	18,856

В таблице 1 приняты следующие обозначения:

1) К_С - отношение «Е_{свз}(В)»/«Е_{свз}(L')» в каждом частотном лепестке, полученный из протокола специальных исследований (СИ) с САИС «Сигурд», дБ;

2) К'_{Ф1} и К_{Ф1} - коэффициенты затухания полученные по формуле (1) с выделением «чистого» шума и без, дБ;

3) К'_{Ф6} и К_{Ф6} - коэффициенты затухания полученные по формуле (6) с выделением «чистого» шума и без, дБ;

4) К_{ГСС} - коэффициент затухания полученный при измерениях на частотах гармоник тестового сигнала с использованием генератора синусоидального сигнала, дБ(мкВ/м).

При вычислении значения К_{ГСС} в частотном лепестке при наличии двух гармоник использовалась следующая формула:

$$K_{ГСС} = \frac{\sqrt{(E_1)^2 + (E_2)^2}}{\sqrt{\left(\frac{E_1}{K_1}\right)^2 + \left(\frac{E_2}{K_2}\right)^2}}, \quad (8)$$

где E₁ и E₂ – напряженности электромагнитного поля на частотах гармоник;

K₁ и K₂ – коэффициенты затухания электромагнитного поля на частотах гармоник.

Как видно из таблицы 1 коэффициент К_С в сравнении с коэффициентами К_{Ф1} имеет небольшой разброс значений не более 0,84 дБ. Он обусловлен тем, что в ПО «Сигурд» невозможно одновременно сохранить результаты измерений в точке 1 и точке 2, и поэтому значения в одной из точек в ПО «Сигурд» и файлах значений несколько отличаются. Соответственно можно сделать вывод, что с помощью ПО «Сигурд» можно осуществить расчет затухания в частотном лепестке по формуле (1). Разброс полученных значений не более 1 дБ между коэффициентами К_{Ф1} и К'_{Ф1} свидетельствует о том, что шум от генераторов в первой и во второй точках существенно превосходил объектовый шум.

Разница затухания в частотном лепестке между измерениями на частотах гармоник К_{ГСС} и измерением фильтр к фильтру К'_{Ф1} может составлять более 6 дБ, а при учете формы огибающей энергетического спектра информативного сигнала К'_{Ф6} более 12

дБ, что свидетельствует о не оптимальности метода измерения затухания на частотах гармоник.

Заключение

В данной статье экспериментально подтверждена возможность использования генератора замещения и специализированной автоматизированной измерительной системы «Сигурд» для определения реального затухания сигналов на объекте информатизации.

Использование генератора замещения при проведении специальных исследований по контролю защищенности и оценке принятых мер защиты информации позволяет определить затухание электромагнитного поля во всем частотном лепестке, а не только на частотах гармоник. Такой подход позволяет более полно отразить характеристику затухания электромагнитного поля, при этом существенно увеличивается точность результатов измерений, и сокращается время проведения специальных исследований по контролю защищенности информации от утечки информации за счет побочных электромагнитных излучений.

СПИСОК ЛИТЕРАТУРЫ:

1. Litao Wang, Bin Yu. Research on the compromising electromagnetic emanation from digital signals, International Conference on Automatic Control and Artificial Intelligence(ACAI 2012), January 2012, Pages 1761-1764, DOI: 10.1049/cp.2012.1329.
2. Скрипник Д. Общие вопросы технической защиты информации. [Электронный ресурс] Режим доступа: <https://www.intuit.ru/studies/courses/2291/591/lecture/12702> (дата обращения: 19.12.2017).
3. M. G. Kuhn, Compromising emanations: Eavesdropping risks of computer displays, Technical report UCAM-CL-TR-577 University of Cambridge, Computer Laboratory [Электронный ресурс], Режим доступа: <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf> (дата обращения 24.12.2017).
4. P. Degauque, P. Laly, V. Degardin, M. Lienard and L. Diquelou Compromising Electromagnetic Field Radiated by In-House PLC Lines, IEEE Global Telecommunications Conference, December 2010, Pages 1-5, DOI:10.1109/GLOCOM.2010.5683144.
5. Litao Wang, Bin Yu. Analysis and measurement on the electromagnetic compromising emanations of computer keyboard, 17th International Conference on Computational Intelligence and Security, December 2011, Pages 640-643, DOI: 10.1109/CIS.2011.146.
6. M. G. Kuhn Compromising emanations of LCD TV sets, IEEE Transaction on electromagnetic compatibility, vol. 55, NO 3, June 2013, Pages. 564 – 570, DOI:10.1109/TEM.2013.2252353.
7. И.Ф. Файсханов, А.С. Лучинин Исследование побочных электромагнитных излучений лазерного принтера, XXIII Международная научно-техническая конференция, Ноябрь 2014, Стр. 37-43, URI: http://elar.urfu.ru/bitstream/10995/46437/1/bip_2014_17.pdf
8. L. Nowosielski, M.Wnuk, Compromising emanations from USB 2 interface, Proceedings of PIERS 2014 in Guangzhou, August 2014, Pages 2666–2670.
9. Leszek Nowosielski, Rafal Przesmycki, and Micha Nowosielski Compromising Emanations from VGA and DVI Interface, Progress In Electromagnetic Research Symposium (PIERS), August 2016, Pages 1024 – 1028, DOI:10.1109/PIERS.2016.7734570.
10. Andrey Ivanov, Ivan Reva, Andrey Ushakov Features of identification and the analysis of collateral electromagnetic radiations from USB flash drives, 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE), October 2016, Pages 156-158, DOI:10.1109/APEIE.2016.7806436
11. Degang Sun, Di Wei, Ning Zhang, Zhiqiang Lv, Xi Yin. Network transmission of hidden data using smartphones based on compromising emanations, 7th Asia Pacific International Symposium on Electromagnetic Compatibility (APEMC), May 2016, Pages 190-193, DOI:10.1109/APEMC.2016.7523005
12. Jun Shi, Degang Sun, Abbas Yongacoglu, Meng Zhang, Dong Wei. Computer Recognition Based On the Compromising Emanations Fingerprint, Canadian Conference on Electrical and Computer Engineering (CCECE), May 2016, Pages 1-6, DOI: 10.1109/CCECE.2016.7726724.
13. Rostislav I. Sokolov, Renat R. Abdullin Determined Factor Parameter Analysis for System of Information Recovery from USB-Keyboards Compromising Emanations, International Applied Computational Electromagnetics Society Symposium - Italy (ACES), March 2017, Pages 1-2, DOI:10.23919/ROPACES.2017.7916332.

14. Sokolov R.I., Abdullin R.R., Dolmatov D.A. Development of Synchronization System for Signal Reception and Recovery from USB-Keyboards, 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), January 2016, Pages 1-4, DOI:10.1109/ICIEAM.2016.7911553.
15. Andrey Ivanov, Ivan Reva, Baryshnikov Yaroslav Development of Hardware-software Complex for Automatized Compromising Electromagnetic Emanation Search, 11th International Forum on Strategic Technology (IFOST), June 2016, Pages 1-3, DOI:10.1109/IFOST.2016.7884180.

REFERENCES:

- [1] Litao Wang, Bin Yu. Research on the compromising electromagnetic emanation from digital signals, International Conference on Automatic Control and Artificial Intelligence (ACAI 2012), January 2012, Pages 1761-1764, DOI: 10.1049/cp.2012.1329.
- [2] Skrypnik D. General issues of technical protection of information. Mode of access: <https://www.intuit.ru/studies/courses/2291/591/lecture/12702> (in Russian).
- [3] M. G. Kuhn, Compromising emanations: Eavesdropping risks of computer displays, Technical report UCAM-CL-TR-577 University of Cambridge, Computer Laboratory Access mode: <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf>.
- [4] P. Degauque, P. Laly, V. Degardin, M. Lienard and L. Diquelou Compromising Electromagnetic Field Radiated by In-House PLC Lines, IEEE Global Telecommunications Conference, December 2010, Pages 1-5, DOI:10.1109/GLOCOM.2010.5683144.
- [5] Litao Wang, Bin Yu. Analysis and measurement on the electromagnetic compromising emanations of computer keyboard, 17th International Conference on Computational Intelligence and Security, December 2011, Pages 640-643, DOI: 10.1109/CIS.2011.146.
- [6] M. G. Kuhn Compromising emanations of LCD TV sets, IEEE Transaction on electromagnetic compatibility, vol. 55, NO 3, June 2013, Pages. 564 – 570, DOI:10.1109/TEMC.2013.2252353.
- [7] I. F. Tashenov, A. S. Luchinin Study of side electromagnetic radiation of the laser printer, the XXIII international scientific-technical conference, November 2014, Pages 37-43, URI: <http://hdl.handle.net/10995/46437> (in Russian).
- [8] L. Nowosielski, M. Wnuk, Compromising emanations from USB 2 interface, Proceedings of PIERS 2014 in Guangzhou ISSN 1559-9450, August 2014, Pages 2666–2670.
- [9] Leszek Nowosielski, Rafal Przesmycki, and Micha Nowosielski Compromising Emanations from VGA and DVI Interface, Progress In Electromagnetic Research Symposium (PIERS), August 2016, Pages 1024 – 1028, DOI:10.1109/PIERS.2016.7734570.
- [10] Andrey Ivanov, Ivan Reva, Andrey Ushakov Features of identification and the analysis of collateral electromagnetic radiations from USB flash drives, 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE), October 2016, Pages 156-158, DOI:10.1109/APEIE.2016.7806436
- [11] Degang Sun, Di Wei, Ning Zhang, Zhiqiang Lv, Xi Yin. Network transmission of hidden data using smartphones based on compromising emanations, 7th Asia Pacific International Symposium on Electromagnetic Compatibility (APEMC), May 2016, Pages 190-193, DOI:10.1109/APEMC.2016.7523005
- [12] Jun Shi, Degang Sun, Abbas Yongacoglu, Meng Zhang, Dong Wei. Computer Recognition Based On the Compromising Emanations Fingerprint, Canadian Conference on Electrical and Computer Engineering (CCECE), May 2016, Pages 1-6, DOI: 10.1109/CCECE.2016.7726724.
- [13] Rostislav I. Sokolov, Renat R. Abdullin Determined Factor Parameter Analysis for System of Information Recovery from USB-Keyboards Compromising Emanations, International Applied Computational Electromagnetics Society Symposium - Italy (ACES), March 2017, Pages 1-2, DOI:10.23919/ROPACES.2017.7916332.
- [14] Sokolov R.I., Abdullin R.R., Dolmatov D.A. Development of Synchronization System for Signal Reception and Recovery from USB-Keyboards 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), January 2016, Pages 1-4, DOI:10.1109/ICIEAM.2016.7911553.
- [15] Andrey Ivanov, Ivan Reva, Baryshnikov Yaroslav Development of Hardware-software Complex for Automatized Compromising Electromagnetic Emanation Search, 11th International Forum on Strategic Technology (IFOST), June 2016, Pages 1-3, DOI:10.1109/IFOST.2016.7884180.

*Поступила в редакцию – 18 декабря 2017 г. Окончательный вариант – 27 апреля 2018 г.
Received – December 18, 2017. The final version – April 27, 2018.*