УДК 004.9

А.И. Подколенко, А.М. Бонч-Бруевич, А.В. Альбовский, Н.А. Егоров

Влияние нестабильности частоты ПЭМИН на возможность оптимального приема сигнала по техническим каналам утечки информации

В статье оцениваются показатели нестабильности частоты интерфейсов персонального компьютера, и приводится сравнение максимального и среднего отклонения центральной частоты интерфейсов VGA и SATA II с действующими Нормами 17-13 «Радиопередатчики всех категорий гражданского применения. Требования на допустимые отклонения частоты».

Ключевые слова: нестабильность частоты, побочные электромагнитные излучения и наводки (ПЭМИН), амплитудная модуляция, тестовые сигналы, отклонение частоты

Введение

Теория оптимального приема сигналов играет важную роль в вопросах передачи информации. Сигнал в процессе следования от передатчика к приемнику подвергается воздействию различных искажающих факторов и помех, поэтому прием сигнала – это получение полезной информации в совокупности с различными шумами и помехами.

Основная задача системы электрической связи (передачи сигналов) – передать информацию от источника к потребителю по линии связи с наименьшими искажениями. Система электрической связи имеет три основные составляющие: передающее устройство, линию связи, приемное устройство (рис. 1).

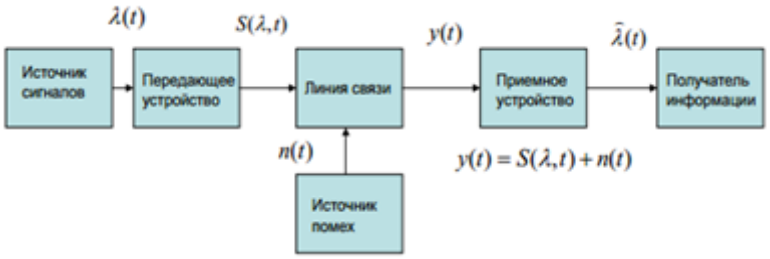

Рис. 1. Структурная схема системы связи

Передающее устройство преобразует первичный сигнал (сообщение) в сигнал-переносчик, способный распространяться по линии связи. Основным устройством передатчика является модулятор. При распространении по линии связи на модулированный сигнал-переносчик воздействует помеха, которая вносит искажения в сообщение. Основной задачей приемного устройства является демодуляция. На выходе приемника имеет место оценка сообщения (точно воспроизвести первичный сигнал невозможно из-за внешних и внутренних помех, а также методических искажений, которые вносятся в процессе передачи сообщения) [1].

Настройка приемника

Первоначально нужно осуществить настройку полосы частот, которую принимает приемник. В данную полосу попадает не только различное количество сигналов, но и множество шумов и помех. Исходя из этого, необходимо правильно настроить приемник под поставленные задачи, что и входит в теорию оптимального приема сигналов.

Оптимальным приемником будет являться тот приемник, который синхронизирован по параметрам сигнала, таким как частота, время, фаза и другим с устройством передачи в каждый данный момент времени. Разумеется, такой приемник – абстракция, так как в реальности на сигнал передат-

чика воздействуют различные виды помех и искажений, и таким образом принятый сигнал будет отличаться от переданного сигнала.

В качестве примера можно привести обыкновенный радиоприемник. Пусть на частоте F вещает необходимая слушателю FM-радиостанция, тогда для корректного приема сигнала слушателю нужно будет установить на приемнике нужную частоту и вид модуляции. В этом случае прием сигнала будет максимально приближен к оптимальному, но при выборе частоты с отклонением $F \pm \Delta f$ или выборе иного вида модуляции качество воспроизводимого сигнала ухудшится.

Условия оптимального приема сигналов

Теория оптимального принятия сигналов напрямую связана с защитой информации. Вследствие того, что технический канал утечки информации (далее – ТКУИ), где происходит радиопередача, состоит из тех же компонентов и отражает полное сходство с системой, где есть приемник, среда и передатчик. При внедрении закладных устройств мы будем получать априорно известную информацию о передаче данных. Зная эту информацию, мы получаем практически идеальный приемник, и ТКУИ приближается к идеализированному случаю, но за некоторым исключением. Мы не можем с полной уверенностью утверждать, что сигнал принят «идеально», так как существует вероятность, что частота генерации сигнала, может быть нестабильной и негативное явление девиации частоты не позволит нам когерентно накапливать сигнал.

Когерентные сигналы – сигналы, имеющие одинаковую частоту и колебания, в которых совершаются вдоль одного и того же направления. Когерентными могут быть не только равные частоты, но и частоты F_1 и F_2, относящиеся друг к другу как отношение натуральных чисел M и N: $F_1/F_2 = M/N$, где $N \neq 0$, поскольку такие частоты при взаимодействии также дают стационарную интерференционную картину [2].

В технической системе когерентная частота сигнала по отношению к частоте сигнала опорного генератора может быть получена:

- постоянной задержкой сигнала опорной частоты;
- делением частоты опорного генератора посредством счётной схемы деления частоты;
- синтезом частоты системой с фазовой автоподстройки частоты (ФАПЧ) или другим методом синтеза, основанным на исходных когерентных частотах.

Применяя способ когерентного накопления, мы можем усилить сигнал и уменьшить влияние шумов, так как полезный сигнал и шумы усиливаются в разных пропорциях. Если мы можем заложить сигнал, у которого угловое вращение будет близко к стабильным показателям, то получается усиление и увеличение зоны обнаружения требуемого сигнала.

Угловая перестройка частоты, которая может возникать в случае девиации радиочастоты (наибольшее отклонение частоты модулированного радиосигнала при частотной модуляции от значения его несущей частоты [3]), может повлиять на когерентное накопление сигнала. Таким образом, представляет интерес выявить данное ограничение для отдельных интерфейсов и оценить возможности ТКУИ, по отношению к когерентному накоплению времени накопление сигнала.

Взаимосвязь между теорией оптимального приема сигналов и поставленной задачей

Со стороны злоумышленника стоит задача зафиксировать опасный сигнал от средства вычислительной техники (далее – СВТ), который формируется в виде узкополосного сигнала, с вероятностью близкой к единице. При этом существует несколько способов фиксации сигнала и связанные с этими способами ограничения:

- когерентное накопление (ограничивается объемом передаваемой информации, чем больше сигналов суммируется для достоверного приема информации, тем меньше информации получает злоумышленник);
- усиление уровня передачи сигнала (достигается путем уменьшения расстояния между СВТ и средством разведки;
- суммирование всех гармоник, которые создаются при формировании и передаче опасного сигнала (ограничивается возможностью СВТ).

При формировании опасного сигнала СВТ представляет собой генератор, характеристики которого влияют на качество принятого сигнала. Одной из таких характеристик является стабильность передачи частоты формированного сигнала. При работе СВТ нагревается, что приводит к возможно-

му изменению выходных результатов. Более того, существуют различные факторы, которые могут приводить к изменению уровня передаваемого сигнала или частоты.

Описание установки и методики проведения измерения

Для измерений использовались следующие приборы:

- анализатор спектра FSWR с диапазоном частот от 10 Гц до 13,6 ГГц;
- анализатор спектра FSU с диапазоном частот от 10 Гц до 43 ГГц;
- измерительная активная антенна АИ5-0, работающая в диапазоне от 0,009–2000 МГц;
- автоматизированное рабочее место (далее – АРМ) в комплект которого входят: системный блок, монитор и USB-накопитель.

На рис. 2 представлена блок-схема измерительной установки.

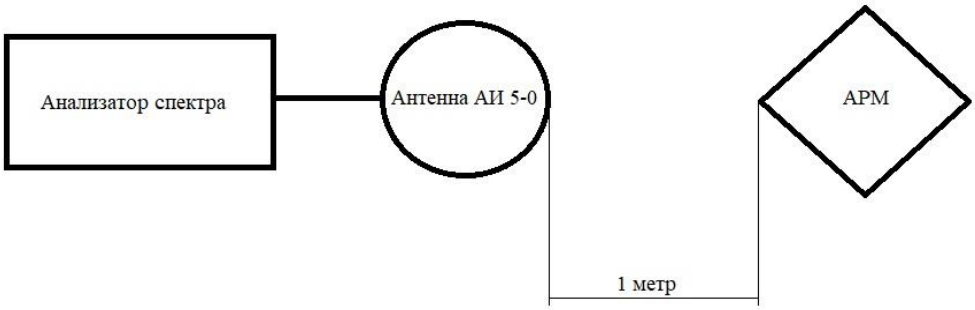

Рис. 2. Блок-схема измерительной установки

Анализатор спектра подключается к антенне АИ 5-0 напрямую. Антенна устанавливается на расстояние 1 метра от исследуемого АРМ. Измерение производится в течение длительного времени (от 45 минут и до 3 часов) после каждого измерения СВТ выключается на 30 минут, чтобы максимально снизить тепловые влияния.

Измерение частоты ПЭМИН интерфейса VGA показало, что при одинаковых настройках анализатора с течением времени частота обнаружения сигнала ПЭМИН изменилась на 21 Гц, что можно видеть на рис. 3.

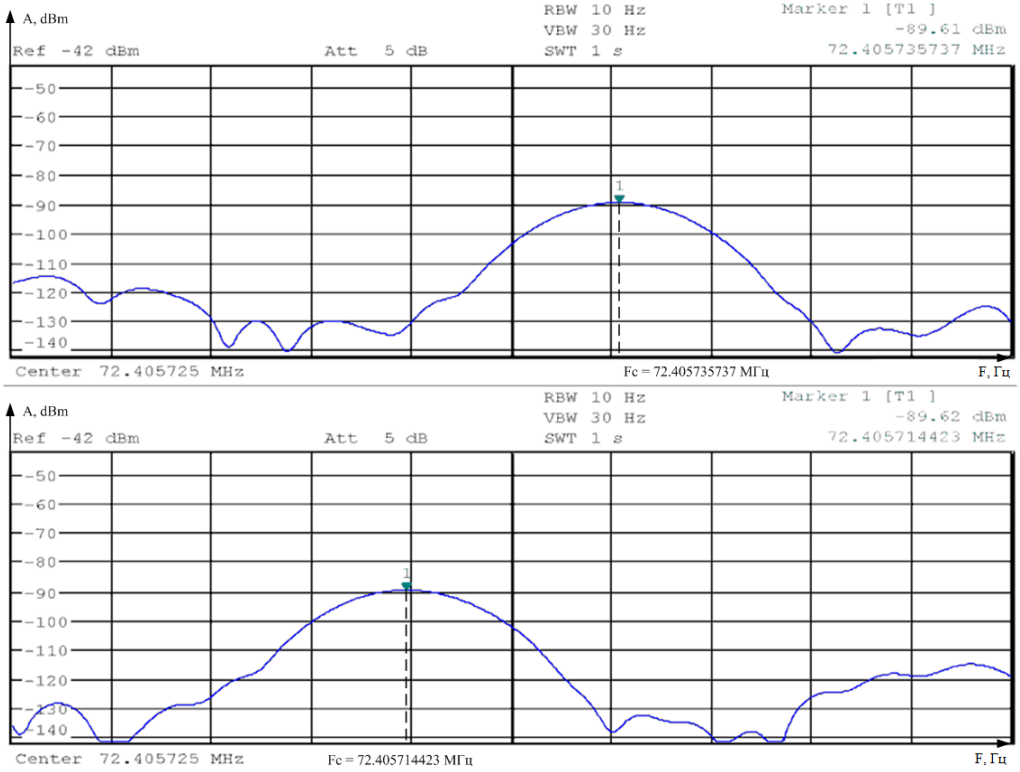

Рис. 3. Отклонение частоты ПЭМИН на 21 Гц

Отсюда следует, что частота сигнала поменялась под действием внешних факторов. Значит можно сделать вывод о том, что нестабильность проявляется для сигналов в ТКУИ ПЭМИН. В табл. 1 приведены результаты проведенных экспериментов с нестабильностью частоты.

Таблица 1

Полученные результаты проведения экспериментов

Тип интерфейса	Кол-во независимых измерений	Среднее время для перестройки на 1 Гц: $T_{1\ Гц}$, с	Средняя скорость перестройки частоты: $U_{ср.}$, Гц/с
VGA (не экранированный)	10	420	0,005
VGA (экранированный)	10	370,2857	0,006
USB 2.0	10	61,2093	0,029
SATA II	10	0,6034	1,65

Относительное изменение частоты высокостабильных генераторов составляет 10^{-11}–10^{-10}. Это означает, что отношение:

$$\frac{\Delta f}{f} = 10^{-10},$$

где Δf – отклонение частоты (Гц), f – несущая частота.

При частоте несущего колебания порядка 1,5 ГГц отклонение частоты на $\Delta f = 1$ Гц составляет $6.7 \cdot 10^{-10}$. Для более наглядного представления применим выражение отклонения частоты в виде миллионных долей (ppm), то есть отклонение на 1 Гц на частоте 1,5 ГГц составит 0,0067.

Известно, что у источников частоты сигналов имеются два вида нестабильности колебаний: долговременная, вызванная систематическим изменением частоты за длительное время; кратковременная, определяемая флуктуационными (быстрыми) изменениями частоты.

Долговременная нестабильность описывает изменения частоты, которые имеют место в течение длительного интервала времени: это отношение ухода частоты к ее номинальному значению за минуту, час, сутки, месяц, год. Кратковременная нестабильность — это относительные флуктуации значения выходной частоты за временной промежуток, который измеряется секундами или долями секунды. Граница между долговременной и кратковременной нестабильностями наиболее часто принимается равной одной или нескольким секундам.

Для оценки кратковременной нестабильности частоты используем метрику – относительную вариацию Аллана (среднеквадратическое двухвыборочное отклонение):

$$\delta f(\tau) = \frac{\sqrt{\sum_{i=1}^{M-1}\left(f(i+1) - f(i)\right)^2/(2(M-1))}}{f_0},$$

где M – число измерений частоты, $f(i)$ – выборка частот, f_0 – номинальное значение частоты, τ – интервал времени между отчетами.

Согласно Нормам 17-13 [3, 4] для радиопередающих устройств, работающих в диапазоне частот 470–2400 МГц мощностью менее 100 Вт, допустимая нестабильность частоты составляет от 10^{-4} для вещательных станций, а для базовых станций стандарта LTE нестабильность может быть до 10^{-7}.

Также требования к нестабильности частоты зависят от вида модуляции, – чем сложнее модуляция, тем выше требования, например, для передатчиков DVB-T, работающих в диапазоне частот 470–862 МГц, допустимое отклонение частоты составляет 1 Гц.

Высокая стабильность частоты требуется для возможности обнаружения и демодуляции сигналов радиосвязи. В задачах обеспечения безопасности схожая проблема возникает при обнаружении и идентификации радиосигналов ПЭМИН. Чем выше стабильность частоты сигнала ПЭМИН, тем проще обнаружить такой сигнал, так как можно обеспечить лучшее отношение сигнал-шум.

Для оценки влияния нестабильности частоты на возможность обнаружения сигнала ПЭМИН были проведены измерения максимального и среднего отклонения частоты на интервале времени 5 минут для следующих интерфейсов ЭВМ – видео (VGA) и жесткий диск SATA. Полученные результаты приведены в табл. 2.

Высокая стабильность частоты сигналов ПЭМИН обусловлена тем, что сигналы внутренних интерфейсов ЭВМ формируется на основе кварцевого резонатора.

Нестабильность частоты по-разному влияет на возможность обнаружения тестового сигнала ПЭМИН и на возможность ведения разведки ПЭМИН. Тестовые сигналы формируются в аппаратуре специальным образом, так чтобы последовательность импульсов, передаваемых через интерфейс, была бы максимально похожа на меандр. Это обеспечивает максимально узкополосный спектр сигнала, который может быть легко обнаружен при проведении работ по оценке уровня сигнала ПЭМИН. Медленные изменения несущей частоты, обусловленные долговременной нестабильностью (по сравнению с длительностью тактовых импульсов), вызывают паразитную амплитудную модуляцию сигнала на входе детектора.

Таблица 2

Результаты измерения максимального и среднего отклонения частоты

Интерфейс	Центральная частота, МГц	Максимальное отклонение частоты, Гц	Среднее отклонение частоты, Гц	Относительное отклонение
VGA	267	5	2	$2 \cdot 10^{-8}$
SATA	1498	60	15	$4 \cdot 10^{-8}$

Выводы

Проанализировав полученные данные, можно сказать о том, что при использовании активных помех на определенных частотах с учетом дестабилизирующих факторов, влияющих на тактовую частоту, присутствует вероятность перехвата сигнала на смещённой во времени частоте, которую активная помеха не сможет покрыть. Значит, применение активных помех будет являться нецелесообразным.

Проведенные исследования также показывают, что наиболее уязвимым к изменению частоты сигнала ПЭМИН является SATA интерфейс, так как наблюдается наиболее сильное амплитудное отклонение частоты равное 400 Гц. Наименее уязвимым будет являться интерфейс VGA. Отклонение при его применении будет равно около 7 Гц.

Список литературы

1. Журавлева Л.М. Теория передачи сигналов: Учебное пособие. – М.: РУТ (МИИТ), 2017. – 149 с.
2. Нормы 17-13. Радиопередатчики всех категорий гражданского применения. Требования на допустимые отклонения частоты.
3. ГОСТ 24375-80. Радиосвязь. Термины и определения.
4. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

ФГУП «Всероссийский научно-исследовательский институт им. Н.Л. Духова» (ФГУП «ВНИИА им. Н.Л. Духова»), 127055, Россия, Москва, ул. Сущевская, 22, тел.: (499) 978-90-99; podkol2007@rambler.ru.

Авторы

Подколенко Антон Игоревич, инженер СНИО, ФГУП «ВНИИА им. Н.Л. Духова»;
тел.: (499) 978-90-99; e-mail: podkol2007@rambler.ru.
Бонч-Бруевич Андрей Михайлович, доцент, к.т.н., МГТУ им. Н.Э. Баумана;
тел.: (499) 978-90-99; e-mail: 123andryb@mail.ru.
Альбовский Александр Владимирович, студент кафедры ИУ10, МГТУ им. Н.Э. Баумана;
тел.: (977) 965-62-50
Егоров Никита Андреевич, студент кафедры ИУ10, МГТУ им. Н.Э. Баумана,
e-mail: kuzya@kuzya.su

A.I. Podkolenko, A.M. Bonch-Bruevich, A.V. Albovskiy, N.A. Egorov

Impact of frequency instability TEMPEST on the possibility of optimal signal reception technical leaks

The article evaluates the indicators of frequency instability of the interfaces of a personal computer, and compares the maximum and average deviations of the center frequency of the interfaces VGA and

SATA II with applicable standards 17-13 «Radio transmitters of all categories of civilian use. Frequency tolerance requirements».

Key words: frequency instability, frequency deviation, Transient Electromagnetic Pulse Emanation Standard (TEMPEST), compromising emanation, amplitude modulation, test signals.

A.I. Podkolenko, A.M. Bonch-Bruevich, A.V. Albovskiy, N.A. Egorov

Impact of Frequency Instability TEMPEST on the Possibility of Optimal Signal Reception Technical Leaks

Abstract. The article evaluates the indicators of frequency instability of the interfaces of a personal computer, and compares the maximum and average deviations of the center frequency of the interfaces VGA and SATA II with applicable standards 17-13 «Radio transmitters of all categories of civilian use. Frequency tolerance requirements».

Key words: frequency instability, frequency deviation, Transient Electromagnetic Pulse Emanation Standard (TEMPEST), compromising emanation, amplitude modulation, test signals.

References

1. Zhuravleva L.M. *Teorya peredachi signalov*: *Uchebnoe Posobie* [Signaling theory: Tutorial]. Moscow, RUT (MIIT), 2017. 149 p. (In Russian)
2. Norms 17-13. Radio transmitters of civilian use. Frequency tolerance requiements. Moscow, AO Kodeks., 2013. 23 p. (In Russian)
3. State Standard 24375-80. Radio communication. Terms and definitions. Moscow, Standartinform Publ., 2005. 44 p. (In Russian)
4. State Standard 53114-2008. Protection of information. Information security provision in organization. Basic terms and definitions. Moscow, Standartinform Publ., 2018. 20 p. (In Russian)

FSUP «All-Russia Research Institute of Automatics» (FSUP VNIIA), State Atomic Energy Corporation Rosatom, ul. Sushchevskaya, 22, 127055 Moscow, Russian Federation.

Authors

Podkolenko Anton Igorevich, engineer, FSUP VNIIA; phone: (499) 978-90-99; e-mail: podkol2007@rambler.ru.

Bonch-Bruevich Andrey Michailovich, docent, candidate of technical sciences, BMSTU; phone: (499) 978-90-99; e-mail: 123andryb@mail.ru.

Albovskiy Alexander Vladimirovich, student IU10, BMSTU; phone: (977) 965-62-50;

Egorov Nikita Andreevich, student IU10, BMSTU, e-mail: kuzya@kuzya.su.