*УДК 621.396*

# ИССЛЕДОВАНИЕ СИСТЕМЫ СИНХРОНИЗАЦИИ ПРИ ВОССТАНОВЛЕНИИ СИГНАЛОВ ПЭМИ USB КЛАВИАТУРЫ В УСЛОВИЯХ ИНДУСТРИАЛЬНОГО ШУМА

© 2016 Д.В. Астрецов, Р.И. Соколов

Уральский федеральный университет, г. Екатеринбург

Статья поступила в редакцию 20.09.2016

В статье разработана система автоподстройки (синхронизации) при приеме сигнала побочного электромагнитного излучения клавиатуры интерфейса USB в условиях негауссовской помехи. В качестве негауссовских помех рассматриваются дискретные случайные процессы, имеющие распределения группы Джонсона, которыми можно аппроксимировать большинство законов распределения реальных индустриальных шумов. Синтезированная система состоит из трех взаимосвязанных частей: блок записи смеси сигнала и помехи при грубом выделении сигнала через коррелятор; блок оптимального восстановления сигнала, состоящего из оптимального приемного алгоритма по критерию минимума среднего риска; блок точного выделения сигнала на основе второго коррелятора. Синтезированная система реализована в виде цифровой модели в программе LabView. Проведен цифровой эксперимент по оценке качества работоспособности системы при восстановлении информативного сигнала ПЭМИ USB клавиатуры, содержащего данные о нажатии клавиши в смеси с помехами Джонсона, в сравнении с существующей системой обнаружения сигнала по максимуму ВКФ на выходе коррелятора.

Ключевые слова: *система автоподстройки, оптимальное восстановление, сигнал ПЭМИ, клавиатура USB, система синхронизации, оптимальный прием*

В открытой отечественной печати не удалось обнаружить информацию о реализации приемных алгоритмов, позволяющих восстанавливать информативные пакеты из ПЭМИ проводных клавиатур интерфейса USB, при этом существуют алгоритмы и системы для обнаружения информативной составляющей в спектральном составе ПЭМИ [1, 3, 4]. Однако исследования в спектральной области не позволяют отличить даже тип пакетов, и, соответственно, данные о клавише. Данный факт обусловлен следующим. Во-первых, пакеты опроса и ответа излучаются с периодичностью 1 мс, а пакеты с данными не периодически с частотой нажатия клавиши (1-2 раза в секунду), то есть пакеты ответа без данных передаются в 1000 раз чаще, чем информационные пакеты. Во-вторых, спектр периодически передаваемых пакетов опроса и ответа без данных шире, чем спектр передаваемых пакетов опроса и ответа с данными. Два эти фактора делают практически невозможным наблюдение спектральной составляющей информационного пакета ответа в режиме работы анализатора спектра в реальном времени [2].

Таким образом, актуальной задачей является разработка специальных алгоритмов обработки информации и экспериментальное установление возможностей их практической реализации с целью определения степени опасности утечки информации по каналам ПЭМИ клавиатур USB в условиях индустриального шума. Поскольку реальные распределения непреднамеренных помех априорно известны, использованы помехи, имеющие одно из трех видов распределений Джонсона, выбор параметров которых позволяет сформировать достаточно широкий класс распределений, близких к распределениям реальных помех.

*Астрецов Дмитрий Вячеславович, кандидат технических наук, профессор. E-mail: dv_astr@mail.ru*
*Соколов Ростислав Игоревич, ведущий инженер. E-mail: rostik-king@yandex.ru*

**Синтез оптимального приемника.** Задача формирования алгоритма оптимального приёма сигнала ПЭМИ в сумме с гауссовской помехой решается при следующих основных допущениях:

1. Сигнал представляет собой последовательность перепадов фронтов в начале каждого импульса, параметры которых (амплитуда, длительность, период следования) известны за исключением сообщения $\lambda(t)$;

2. Помеха является дискретной последовательностью, совпадающих по времени с дискретами сигнала, имеющими один из трех законов распределения мгновенных значений Джонсона, её интенсивность велика, так что отношение импульсных мощностей одиночных сигналов и помехи намного меньше единицы, поэтому для надежного выделения информации используется накопление сигнала;

3. В качестве критерия оптимальности используется критерий минимума среднего риска при простой функции потерь, следовательно, в качестве оптимального правила решения может быть использован алгоритм максимума апостериорной плотности вероятности в виде

отношения правдоподобия. При таком критерии оптимальный приём обеспечивает минимум полной вероятности ошибки [7].

На вход приемника поступает сигнал $y(t)$, определяемый уравнением (1):

$$y(t) = s(t) + \xi(t) + n(t), \quad (1)$$

где $s(t)$ – полезный сигнал, определяемый как последовательность видеоимпульсов; $\xi(t)$ – помеха, заданная одной из плотностей распределения Джонсона; $n(t)$ – нормальный внутренний шум приемника.

В результате моделирования отношения правдоподобия – отношения плотности распределения смеси сигнала и помехи к плотности распределения помехи [5, 6] получаем выражение (2) для реализации приемного алгоритма, представленного на рис. 1:

$$l_m = \frac{1}{\sigma_z^2(1-R^2)}\sum_{i=0}^{m-1}[(Q(y_{i+1}) - Q(y_i)R][s_{i+1}Q'(y_{i+1}) - s_iQ'(y_i)R] + \sum_{i=0}^{m-1} s_{i+1}\frac{Q''(y_{i+1})}{Q'(y_{i+1})} \quad (2)$$

Помеха представляется случайным процесссом $\xi$, который можно описать как результат безынерционного преобразования $q(z_i)$ марковского гауссова процесса $z_i$, для которого существует обратная функция $Q=q^{-1}$, так что $z_i = Q(\xi)$. Процесс $z_i$ задан начальной и условной плотностями распределения вероятностей с коэффициентом корреляции $R$ и дисперсией $\sigma_z^2$.

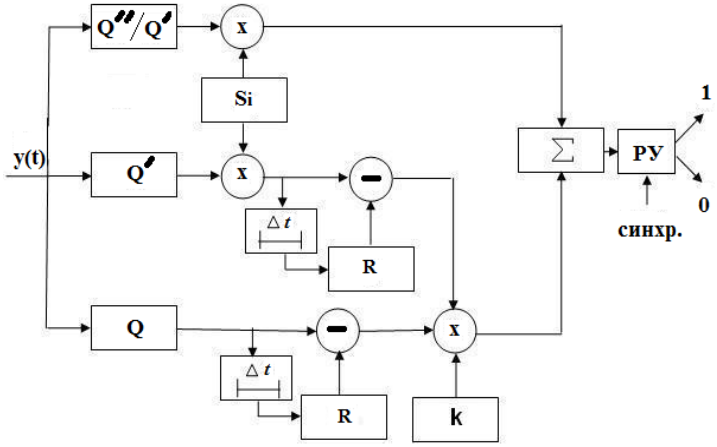


**Рис. 1.** Блок-схема оптимального приемника

Подставляя в общее выражение (2) частные нелинейные преобразования, получим выражения, определяющие модели оптимального приема для разных видов помех. Например, (3) определяет структуру оптимального приемника для $S_L$-распределённой помехи, а (4) – для $S_B$-распределённой помехи:

$$l_m = \sum_{i=1}^{m}\frac{((\gamma+\eta\ln(y_{i+1})) - (\gamma+\eta\ln(y_i))R)^2}{2\sigma_z^2(1-R^2)} - \sum_{i=1}^{m}\frac{((\gamma+\eta\ln(y_{i+1}-s_{i+1})) - (\gamma+\eta\ln(y_i-s_i))R)^2}{2\sigma_z^2(1-R^2)} + \sum_{i=1}^{m}\ln\frac{|y_i|}{|y_i-s_i|} \quad (3)$$

**Синтез алгоритма синхронизации.** Работа оптимального приемника возможна только при точной синхронизации первого отсчета принятого пакета с первым отсчетом опорного сигнала. Для реализации алгоритма восстановления необходимо на первом этапе выделить пакет из всей последовательности, поступающей на вход приемного устройства. Для этого используется коррелятор, настроенный на информационный пакет.

$$l_m = \sum_{k=1}^{m}\frac{\left(\ln\left(\frac{y_{k+1}}{1-y_{k+1}}\right) - \ln\left(\frac{y_k}{1-y_k}\right)R\right)^2}{2\sigma_z^2(1-R^2)} - \sum_{k=1}^{m}\frac{\left(\ln\left(\frac{y_{k+1}-s_{k+1}}{1-y_{k+1}-s_{k+1}}\right) - \ln\left(\frac{y_k-s_k}{1-y_k-s_k}\right)R\right)^2}{2\sigma_z^2(1-R^2)} + \sum_{k=1}^{m}\frac{|y_k(y_k-s_k)|}{|(y_k-s_k)(1-y_k+s_k)|} \quad (4)$$

Вследствие излучения в пространство перепадов уровней импульсов (фронтов), а не самих импульсов, протекающих по информационному кабелю интерфейса USB клавиатуры, сложной задачей является формирование опорного сигнала коррелятора при перехвате излучения с возможностью восстановления информативного пакета. Весьма затруднительно создать математическую модель сигнала ПЭМИ клавиатуры, реализуемую методами визуального программирования, для генерации в оптимальном приемнике

как опорного сигнала. Поэтому в качестве опорного сигнала используются записанные в условиях минимального внешнего шума сигналы ПЭМИ пакетов данных, содержащих информативные данные о нажатии каждой клавиши клавиатуры.

На первом этапе обработки сигнал ПЭМИ в смеси с шумом проходит через корреляторы, настроенные на каждый пакет данных. На выходе наблюдаются ВКФ каждого пакета сообщения и опорного пакета. При совпадении пакетов ВКФ имеет ярко выраженный максимум для данных снятых с одного информационного кабеля (рис. 2 и 3). Затем происходит определение точки максимума взаимной корреляционной функции и выделение одиночного пакета, по априорно известному количеству отсчетов (4500 отсчетов), приходящихся на один пакет. Таким образом, нахождение точки максимума ВКФ является грубой синхронизацией для последующей обработки выделенного пакета из сообщения с помощью оптимального приемного алгоритма.

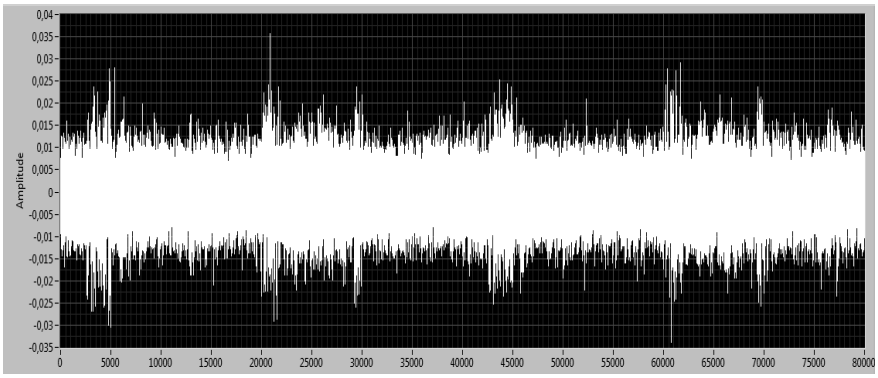


**Рис. 2.** Смесь информационного сообщения ПЭМИ и $S_B$ помехой Джонсона на входе коррелятора настроенного на клавишу «Q»

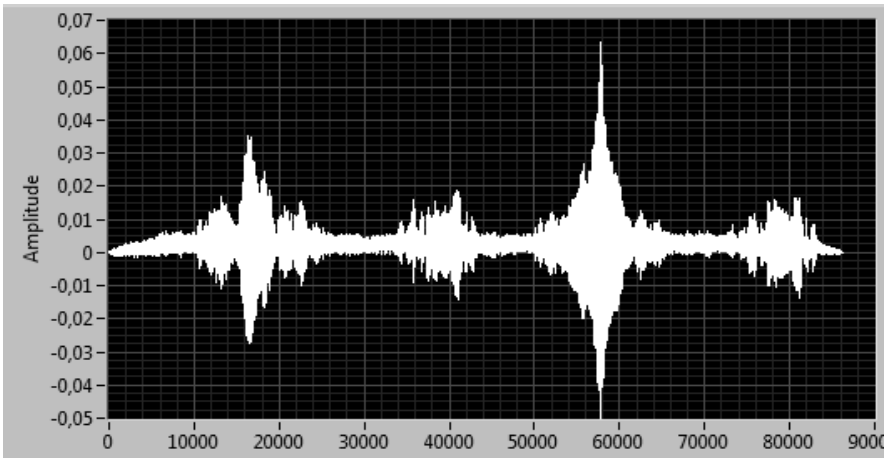


**Рис. 3.** ВКФ на выходе коррелятора для сигналов снятых с одного информационного провода при С/Ш -5 дБ

На втором этапе выделенная последовательность подвергается восстановлению в оптимальном приемнике по схеме 1. При этом синхронизация существенно влияет на качество восстановления, однако из-за наличия шума точка максимума ВКФ смещается относительно истинного положения начала пакета на случайное число отсчетов (но не более 67, так как на один импульс приходится 67 отсчетов). Поэтому для повышения точности восстановления сигнала вводится автоматическая подстройка, при которой выделенная последовательность подается на вход оптимального приемника (рис. 5), несколько раз смещая свое начала на один такт (67 раз со смещением на 1 отсчет), до полной синхронизации с опорным сигналом. На выходе оптимального приемника расположен второй коррелятор, настроенный на точно засинхронизированный сигнал (рис. 6). В качестве опорного сигнала берется восстановленный пакет из смеси с минимальным присутствием шума, для которого априорно известно время прихода первого импульса (идеальная синхронизация). Полная схема системы восстановления с синхронизацией представлена на рис. 4. На выходе коррелятора 2 происходит определение максимума из 67 взаимных корреляционных функций и выделение восстановленного пакета, наиболее полно совпадающего с пакетом идеальной синхронизации.

**Результаты эксперимента.** В результате проведенного эксперимента были получены графики зависимости нормированных значений взаимно-корреляционной функции (НВКФ) от отношения С/Ш в условиях помех Джонсона для приемника с использованием системы автоподстройки (синхронизации) и без использования, представленные на рис. 7.

Использование разработанного алгоритма восстановления сигнала осуществимо в условиях априорно неизвестных параметрах о сигнале и помехах. В частности нет необходимости точно знать время прихода первого импульса при мощностях помех с отношением С/Ш больше -3 дБ для *SL* и *SU* помех Джонсона и больше -10 для *SB* помехи Джонсона для достижения качества восстановления определяемого вероятностью ошибки правильного восстановления $P_{ош}$ равной 0,1 (рис. 7).

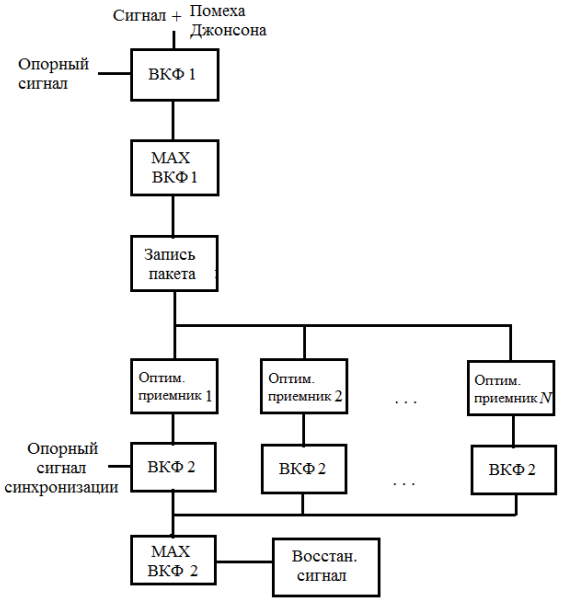


**Рис. 4.** Блок-схема системы синхронизации и восстановления сигнала ПЭМИ

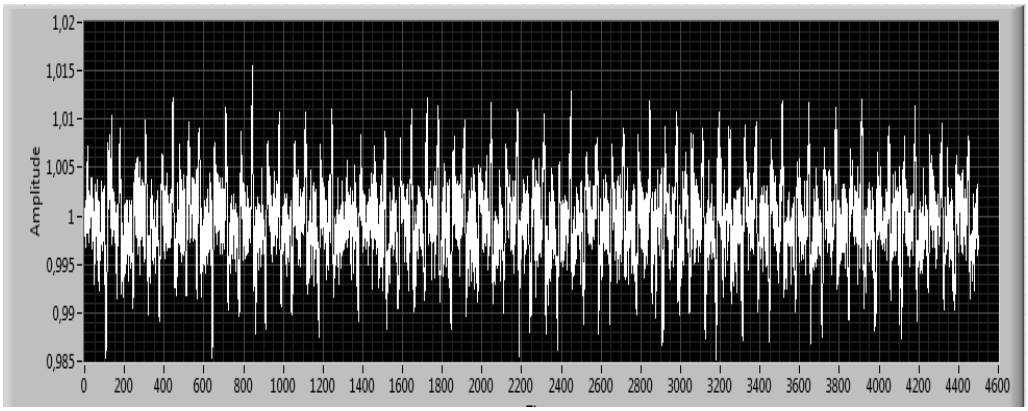


**Рис. 5.** Сигнал ПЭМИ USB-клавиатуры в смеси с SL помехой Джонсона при С/Ш 0дБ на входе системы автоматической подстройки синхронизации

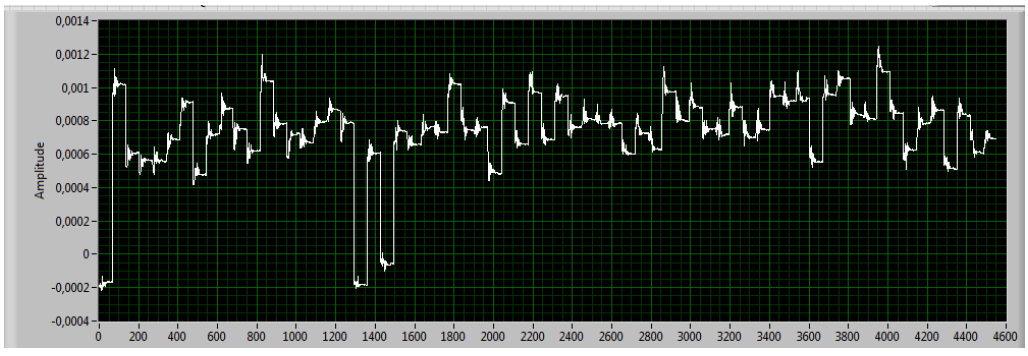


**Рис. 6.** Восстановленный сигнал на выходе системы автоматической подстройки синхронизации по максимальному значению ВКФ и график ВКФ

**Выводы:**

1. Использование синхронизации и выделения пакета по максимальному значению ВКФ принятого сигнала и опорного дает возможность восстановления данных для различных сигналов и помех.

2. Использование автоматической подстройки синхронизации по максимальному значению ВКФ восстановленного сигнала и опорного сигнала идеальной синхронизации позволяет повысить возможности восстановления для приемного алгоритма на 3-6 дБ для различных помех Джонсона, однако это приводит к некоторому

росту времени обработки, что может затруднить осуществление обработки в режиме реального времени.

3. *SB* помеха Джонсона обладает наихудшим маскирующим эффектом проигрывая БГШ порядка 10 дБ, при этом помехи *SL* и *SU* сопоставимы по степени маскирующего действия при выбранном алгоритме восстановления и уступают БГШ не более 1-2 дБ.

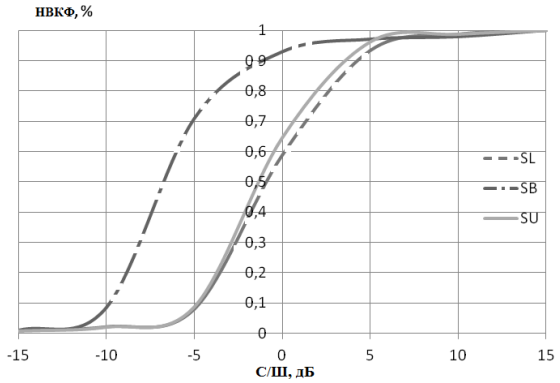


**Рис. 7.** График зависимости нормированных значений взаимно-корреляционной функции НВКФ от отношения С/Ш для различных помех

СПИСОК ЛИТЕРАТУРЫ:

1. *Vuagnoux, M.* Compromising Electromagnetic Emanations of Wired and Wireless Keyboards / *M. Vuagnoux, S. Pasini* // EPFL, Lausanne, Switzerland. http-www. usenix.org-events-sec09-tech-f ull_ papers-vuagnoux. pdf
2. *Kobyakov, V.Yu.* Detection of Tempest Conductors and Connectors when Transferring via USB / *V.Yu. Kobyakov, A.S. Luchinin* // UrFR Newsletter. Security in the information sphere. 2014. No. 14. P. 4-8.
3. *Хорев, А.А.* Оценка возможности перехвата побочных электромагнитных излучений клавиатуры компьютера. – М.: Арсенал СТ, 2005. С. 47-63.
4. *Kuhn, M.G.* Compromising emanations: eavesdropping risks of computer displays // Technical Report UCAM-CL-TR-577, University of Cambridge, Computer Laboratory, December 2003.
5. *Астрецов, Д.В.* Анализ потенциальной помехоустойчивости выделения бинарного сообщения при действии гауссовских и негауссовских помех / *Д.В. Астрецов, Ю.А. Нифонтов, Р.И. Соколов* // Труды XI междун. науч.-техн. конф. «Физика и технические приложения волновых процессов»// под ред. *Мительмана Ю.Е.* – Екатеринбург: Изд. УрФУ, 2012. С. 325-329.
6. *Кендал, М.* Теория распределений, под ред. *А.Н. Колмогорова* / *М. Кендал, А. Стюарт* – М.: Наука, 1966. С. 171.
7. *Гуткин, Л.С.* Теория оптимальных методов радиоприема при флуктуационных помехах – М.: Советское радио, 1972. 447 с.

## STUDY OF SYNCHRONIZATION SYSTEM FOR SIGNAL RECOVERY FROM USB-KEYBOARD COMPROMISING EMANATIONS IN CONDITIONS OF INDUSTRIAL NOISE

© 2016 D.V. Astretsov, R.I. Sokolov

Urals Federal University, Ekaterinburg

An automatic control (recovery) system for reception of USB-Keyboard Compromising Emanations has been developed in condition of non-Gaussian noise. Synthesized system consists of three interconnected parts: the record unit, the optimal recovery unit, and sensitive extraction unit. As the noise both Gaussian and non-Gaussian discrete random processes are considered. Non-Gaussian processes have Johnson distribution and allow approximating accurately the most of distribution laws of really existing artificial processes. The system has been implemented as digital model in LabView software. At the first stage the correlation extracts the signal and defines first sample arrival time. At the second stage synthesized optimal receiver recovers information sequence. It has been proved the use of developed recovering algorithm is feasible under conditions of a priori unknown signal and noise parameters when maximum of cross-correlation function synchronizing.

Key words: *automatic control system, optimal recovery, USB-keyboard, compromising emanations, synchronization system, optimal reception*

*Dmitriy Astretsov, Candidate of Technical Sciences, Professor. E-mail: dv_astr@mail.ru*
*Rostislav Sokolov, Leading Engineer. E-mail: rostik-king@yandex.ru*