На правах рукописи

Соколов Ростислав Игоревич

ИССЛЕДОВАНИЕ АЛГОРИТМОВ ОБРАБОТКИ СИГНАЛОВ ДЛЯ ОБНАРУЖЕНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАТИВНЫХ ДАННЫХ ИЗ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ USB КЛАВИАТУР

Специальность: 05.12.13

Системы, сети и устройства телекоммуникаций

Автореферат

диссертации на соискание ученой степени

кандидата технических наук

Екатеринбург – 2016

Работа выполнена на кафедре радиоэлектронных и телекоммуникационных систем Института радиоэлектроники и информационных технологий Федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет имени первого президента России Б.Н. Ельцина».

Научный руководитель: **Астрецов Дмитрий Вячеславович**
кандидат технических наук, профессор, профессор департамента радиоэлектроники и связи Института радиоэлектроники и информационных технологий Уральского федерального университета

Официальные оппоненты: **Румянцев Константин Евгеньевич**
доктор технических наук, профессор, зав. кафедрой информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности Южного федерального университета

Григоров Игорь Вячеславович
доктор технических наук, доцент, проректор по воспитательной работе и международному сотрудничеству Поволжского государственного университета телекоммуникаций и информатики

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет путей сообщения»

Защита состоится «17» февраля 2017 г. в 14 часов 00 минут на заседании диссертационного совета Д 219.003.02 при Федеральном государственном образовательном бюджетном учреждении высшего образования «Поволжском государственном университете телекоммуникаций и информатики» в конференц-зале корпуса №1 по адресу: ул. Льва Толстого, д. 23, г. Самара.

С диссертацией можно ознакомиться в библиотеке Федерального государственного образовательного бюджетного учреждения высшего образования «Поволжский государственный университет телекоммуникаций и информатики» и на сайте www.psuti.ru/science/diss-ob.

Автореферат разослан «__» _____ 201 г.

Ученый секретарь
диссертационного совета Д 219.003.02,
д.т.н., профессор А.И. Тяжев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

В настоящее время использование электронных устройств в различных системах связи породило проблему защиты информации от утечки по техническим каналам.

Качество приёма сигнала ПЭМИ существенно зависит не только от мощности, но и от вида распределения помехи. Однако автоматизированные комплексы для специальных исследований являются универсальными и не рассчитываются для каждого вида сигнала и помехи. Поэтому для исследования предельных возможностей обнаружения и восстановления сигналов ПЭМИ клавиатур интерфейса USB 1.0 и эффективного радиопротиводействия требуется синтез и моделирование алгоритмов обработки, оптимальных для исследуемых сигналов и помех.

В нормативных документах ФСТЭК описаны методики аттестации ПК и их элементов на предмет опасности утечки информации по каналам ПЭМИ. Однако в документах не рассматриваются особенности характеристик ПЭМИ отдельных элементов персональных компьютеров, в частности клавиатур интерфейса USB, не конкретизируются методики их исследования. Эти обстоятельства требуют уточнения методик аттестационных исследований элементов ПК и указывают на необходимость исследования характеристик ПЭМИ.

Для того чтобы оценить степень защищенности объекта от перехвата побочного электромагнитного излучения, а главное, принять соответствующие меры для защиты объекта, необходимо исследовать потенциальную возможность перехвата информации в зависимости от различных параметров полезного сигнала и электромагнитных условий, в которых эксплуатируется объект защиты, а также от априорных сведений, которыми обладает перехватчик.

Степень разработанности темы исследования

Задачей обнаружения информативных ПЭМИ технических средств и восстановления конфиденциальной информации в настоящее время занимаются ряд российских и зарубежных научных школ. Комплексный подход к проблеме представлен в исследованиях сотрудников факультета РЛА МАИ (НИУ), Кузнецова Ю.В., Бехтина М.А, Горбуновой А.А.и др. В свою очередь, в работах С. Пасини и М. Вано показана возможность перехвата сигнала на значительном расстоянии от клавиатуры.

Исследования возможностей компенсации индустриальных помех при оценке защищенности информации, обрабатываемой техническими средствами, в каналах побочных электромагнитных излучений проведены в рамках научно-исследовательской работы сотрудниками ИРИТ-РТФ УрФУ. Однако в данной работе оценивается качество работы приемников с использованием различных схем компенсаторов помех только для сигналов ПЭМИ PS/2 клавиатуры.

Непосредственно исследования возможностей перехвата сигнала ПЭМИ клавиатур USB интерфейса представлены в работах Хорева А.А., в которых проводиться анализ спектров сигналов ПЭМИ клавиатуры, и обнаруживаются неинформационные спектральные составляющие. При этом представленный метод анализа не позволяет выявить информационные составляющие в спектре побочных электромагнитных излучений USB клавиатуры.

Таким образом, при анализе существующих исследований не удалось обнаружить информацию о реализации приемных алгоритмов, позволяющих обнаруживать и восстанавливать информативные пакеты из ПЭМИ проводных клавиатур интерфейса USB. Следовательно, 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.

Особую актуальность данная проблема приобретает в связи с тем, что перспективные методы обработки сигналов ПЭМИ, а в частности, вейвлет-алгоритм для классификации сигналов сложной формы в каналах побочных излучений систем связи и вычислительной техники при контроле их информационной безопасности, разработанный Королевым С. Н. применим только для стационарного белого гауссовского шума; применение негауссовских помех приводит к существенному ухудшению работы. Таким образом, требуется разработка специальных алгоритмов обработки сигналов, не снижающих качество восстановления сигнала ПЭМИ при действии негауссовских помех.

Цель и задачи исследования

Целью работы является исследование алгоритмов нелинейной фильтрации марковских процессов и алгоритмов оптимального приема по критерию минимума среднего риска для квазислучайного телеграфного сигнала при работе в нестационарном режиме при действии гауссовской и негауссовских помех Джонсона, позволяющих повысить эффективность обнаружения и восстановления сигнала ПЭМИ клавиатуры ПЭВМ интерфейса USB.

Для достижения поставленной цели решаются следующие задачи:

1. Анализ основных свойств сигналов, содержащихся в побочных электромагнитных излучениях.
2. Создание математической модели сигнала и канала связи для синтеза алгоритмов оптимального и квазиоптимального приема.
3. Выбор значений параметров различных помех для наиболее полного охвата реальных помеховых условий.
4. Синтез алгоритмов выделения конфиденциальной информации на основе марковской теории нелинейной фильтрации и теории оптимального приема при действии гауссовских и негауссовских помех.

5. Теоретическое решение уравнений, определяющих схемы оптимального приема по критерию минимума среднего риска для установления маскирующих свойств гауссовских и негауссовских помех.

6. Оценка эффективности разработанных алгоритмов методами математического моделирования и полунатурного эксперимента.

7. Проведение детерминированного факторного анализа на основе полученных зависимостей вероятности ошибки от различных параметров сигнала, помехи и приемного устройства для определения степени влияния каждого фактора.

8. Расчет потенциальной дальности перехвата сигналов ПЭМИ клавиатуры интерфейса USB для определения адекватных мер по защите объектов от утечки информации по каналу побочного электромагнитного излучения.

Научная новизна полученных результатов

В диссертационной работе получены следующие, не встречавшиеся в известной литературе, результаты:

1. Разработаны алгоритмы оптимального приема по критерию минимума среднего риска для квазислучайного телеграфного сигнала, позволяющие восстанавливать данные, содержащиеся в побочном электромагнитном излучении клавиатуры интерфейса USB при действии гауссовской и негауссовских помех Джонсона.

2. Установлены зависимости качества восстановления информативных данных о нажатии клавиш из сигналов ПЭМИ клавиатур интерфейса USB от типа и мощности помехи, имеющей либо гауссовское распределение, либо одно из трех распределений Джонсона с целью определения качества работы синтезированных алгоритмов оптимального приема.

3. Разработаны алгоритм совместной нелинейной фильтрации непрерывных и дискретного марковских процессов и упрощенный алгоритм нелинейной фильтрации двумерных непрерывных марковских процессов, описывающих сигнал побочного электромагнитного излучения клавиатуры ПЭВМ интерфейса USB и помеху с нормальным распределением плотности вероятности или распределением Джонсона для работы в нестационарном режиме, позволяющие повысить качество обнаружения сигнала.

4. Установлены зависимости качества обнаружения информативных и неинформативных данных из сигналов ПЭМИ клавиатур интерфейса USB от типа и мощности помехи, имеющей либо гауссовское распределение, либо одно из трех распределений Джонсона с целью определения качества работы синтезированных алгоритмов нелинейной фильтрации.

Теоретическая и практическая значимость работы

Практическое значение работы состоит в возможности повышения информационной безопасности за счет совершенствования аттестации средств связи и оргтехники при

использовании разработанных алгоритмов обработки информации и выбора наиболее эффективной маскирующей помехи от перехвата информации по каналам ПЭМИ. При этом результаты, обеспечивающие практическую значимость диссертационной работы, использованы в госбюджетной научно-исследовательской работе №6233 ИРИТ-РТФ УрФУ.

Теоретическое значение работы состоит в разработке перспективных алгоритмов оптимального приема и алгоритмов нелинейной фильтрации с возможностью применения в различных радиолокационных, телекоммуникационных, финансовых системах, а также в системах обработки изображений. При этом результаты, обеспечивающие теоретическую значимость диссертационной работы, использованы при выполнении научно-исследовательской работы по теме «Разработка системы обработки данных радиолокатора» для Ключевого центра превосходства УрФУ № 02.A03.21.0006. Также результаты исследования признаны перспективными и могут быть использованы в работе отдела 313 АО "НПО автоматики" для разработки алгоритмов первичной и вторичной обработки информации ГНСС ГЛОНАСС/GPS при проектировании узлов систем спутниковой навигации для перспективных применений, что подтверждается актом внедрения №313/960 от 28.11.2016.

Кроме того, результаты внедрены в учебный процесс в ФГАУО ВПО «УрФУ имени первого Президента России Б.Н.Ельцина» на кафедре радиоэлектронных и телекоммуникационных систем ИРИТ-РТФ, что подтверждается актом внедрения.

Методология и методы исследования

Методы исследований_включают в себя анализ и обобщение теории статистических оценок, теории нелинейной фильтрации марковских процессов, теоретические расчеты с привлечением метода математической индукции, цифровое моделирование синтезированных алгоритмов, экспериментальные исследования с использованием современной ВЧ техники, а так же детерминированный факторный анализ.

Положения выносимые на защиту

Научные положения, выносимые на защиту, в соответствии с п.2 паспорта специальности 05.12.13:

1. Алгоритмы оптимального приема по критерию минимума среднего риска для БГШ, S_L, S_B, S_U помех Джонсона и результаты исследования их применения для восстановления данных, содержащихся в побочном электромагнитном излучении клавиатуры интерфейса USB.

2. Алгоритм совместной нелинейной фильтрации непрерывных и дискретного марковских процессов с тремя состояниями и алгоритм нелинейной фильтрации двумерных непрерывных марковских процессов для работы в нестационарном режиме для фильтрации БГШ, S_L, S_B, S_U помех Джонсона и результаты исследований их применения при обнаружении информативной составляющей, содержащейся в ПЭМИ клавиатур интерфейса USB.

3. Результаты исследований возможностей практического применения разработанных алгоритмов нелинейной фильтрации и оптимального приема для обнаружения и восстановления информативных и неинформативных составляющих сигнала ПЭМИ клавиатуры интерфейса USB в идеальных условиях без воздействия внешнего шума и в реальных условиях при действии БГШ и S_U, S_L и S_B помехи Джонсона.

4. Результаты исследования маскирующих свойств помех, имеющих гауссовское распределение и распределения Джонсона в зависимости от параметров распределений, полученные на основании теоретического решения уравнения для оптимального алгоритма приема по критерию минимума среднего риска для квазислучайного телеграфного сигнала.

Достоверность научных результатов

Достоверность научных положений, выводов и результатов обеспечивается: корректностью используемых современных математических методов, таких как теория статистических оценок, теория нелинейной марковской фильтрации; согласованностью полученных результатов исследования теоретическими расчетами и практическим экспериментом; использованием современной высокочастотной техники, позволяющей провести точные вычисления и имитационное моделирование; апробацией результатов исследований автора на различных международных и всероссийских конференциях.

Апробация работы

Содержание и отдельные положения диссертации докладывались и получили одобрение на 20 различных конференциях, в том числе на XI Международной научно-техническая конференции “Физика и технические приложения волновых процессов” (Екатеринбург, 2012); XI, XII и XIV Всероссийской научно-технической конференции “Безопасность информационного пространства” (Тюмень, 2012, 2015; Екатеринбург, 2013); XVII Всероссийской научно-технической конференции «Информационные технологии и электроника» (Екатеринбург, 2013); XV Международной научно-практической конференции “Современные информационные и электронные технологии” (Украина, Одесса, 2014); XXIV и XXV Международной Крымской конференции “СВЧ-техника и телекоммуникационные технологии” (Севастополь, 2014, 2015); II Международной конференции “Информационные технологии, телекоммуникации и системы управления” (Екатеринбург, 2015); Международной научно-технической конференции “International Conference on Industrial Engineering ICIE 2016” (Челябинск, 2016); на зарубежных международных конференциях: “Conference on Microwaves, Communications, Antennas and Electronic Systems COMCAS 2015” (Тель-Авив, Израиль, 2015); “International Conference on Computational Techniques in Information and Communication Technologies ICCTICT 2016” (Нью Дели, 2016) и др.

Структура и объём работы

Диссертация состоит из введения, 5 глав и заключения, изложенных на 158 страницах машинописного текста, содержит 100 рисунков, 5 таблиц, список литературы из 118 наименований и 2 приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** приводится анализ актуальности исследуемого вопроса. Сформулированы цели и задачи диссертационного исследования, показаны научная новизна и практическая значимость полученных результатов. Приведены научные положения, выносимые на защиту, указаны состав и структура диссертации.

Первая глава является обзорной и заканчивается постановкой задачи исследования. Дается описание работы протокола USB, сигнала ПЭМИ клавиатур интерфейса USB, гауссовских и негауссовских помех, а также делается анализ существующих разработок для решения задачи обнаружения информативных ПЭМИ технических средств и восстановления конфиденциальной информации. Дается научное обоснование актуальности задачи по разработке технических решений, касающихся повышения качества приема сигналов ПЭМИ.

Во **второй главе** разрабатывается структура оптимального приемника по критерию минимума среднего риска для восстановления сигнала ПЭМИ клавиатуры интерфейса USB и рассчитывается влияние типа помехи на качество восстановления.

Оптимальный приемник строится путем моделирования отношения правдоподобия – отношения плотности распределения смеси сигнала и помехи к плотности распределения помехи, определяемого уравнением (2):, при этом на вход приемника поступает сигнал *y(t)*, определяемый уравнением (1):

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

где *s(t)* – полезный сигнал, представляющий собой последовательность перепадов фронтов в начале каждого импульса, параметры которых (амплитуда, длительность, период следования) известны за исключением сообщения $\lambda(t)$; $\xi(t)$ – помеха, заданная одной из плотностей распределения Гаусса или Джонсона; *n(t)* – нормальный внутренний шум приемника.

$$\Lambda_m = \frac{w_0(Q(y_1 - s_1))\left|Q'(y_1 - s_1)\right| \prod_{i=1}^{m-1} (Q(y_{i+1} - s_{i+1}) / Q(y_i - s_i))\left|Q'(y_{i+1} - s_{i+1})\right|}{w_0(Q(y_1))\left|Q'(y_1)\right| \prod_{i=1}^{m-1} (Q(y_{i+1}) / Q(y_i))\left|Q'(y_{i+1})\right|} \qquad (2)$$

На основании решения уравнения (2) получено выражение (3), определяющее схему оптимального приемника, изображенного на рисунке 1:

$$\ln \Lambda_m = \sum_{i=1}^{m} \frac{(Q(y_{i+1}) - Q(y_i)R)^2}{2\sigma_z^2(1-R^2)} - \sum_{i=1}^{m} \frac{(Q(y_{i+1} - s_{i+1}) - Q(y_i - s_i)R)^2}{2\sigma_z^2(1-R^2)} + \sum_{i=1}^{m} \ln \frac{\left|Q'(y_i - s_i)\right|}{\left|Q'(y_i)\right|} \quad (3)$$

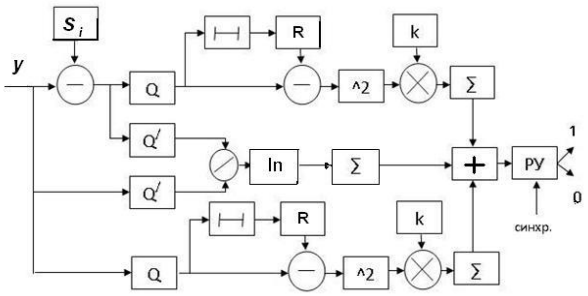

Рис. 1 – Структурная схема оптимального приемника.

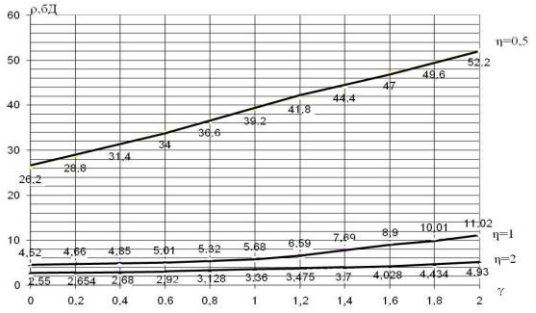

Рис. 2 – Проигрыш в маскирующем действии SU помехи по сравнению с гауссовской.

Проводится теоретический анализ синтезированного оптимального способа приема для оценки помехоустойчивости восстановления информативного путем сравнения вероятности ошибки восстановления сообщения при негауссовских помехах с вероятностью ошибки восстановления сообщения при гауссовской помехе для заданного значения отношения мощностей сигнала и помехи. В результате получены зависимости проигрыша в маскирующем действии помех Джонсона по сравнению с гауссовской (рисунок 2).

В **третей главе** в результате решения задач оптимальной нелинейной фильтрации в гауссовом приближении, выполнен синтез квазиоптимального приемного алгоритма для совместной фильтрации непрерывных и дискретного марковских процессов и упрощенного алгоритма нелинейной фильтрации двумерных непрерывных марковских процессов, описывающих сигнал ПЭМИ клавиатуры USB и помеху, в нестационарном режиме.

Полезное сообщение $\lambda(t)$ и помеха $z(t)$, представляющие марковские процессы, задаются соответствующими априорными стохастическими дифференциальными уравнениями. В результате решения системы ИДУ Стратоновича для совместной фильтрации непрерывных процессов $\lambda(t)$ и $\xi(t)$ и дискретного параметра $\theta(t)$ для случая, когда $\theta(t)$ принимает значения 1,0 или -1, в нестационарном режиме для гауссовского приближения, получена система из 21 нелинейного дифференциального уравнения второго порядка.

Осуществлен синтез схемы обработки для каждого фильтруемого параметра (на рисунке 4 представлен алгоритм нелинейной фильтрации параметра λ_1, заданного уравнением 4), и определен как отдельный блок, после чего блоки объединены в общую структурную схему с необходимыми связями.

$$\frac{d\lambda_1}{dt} = -K_{\lambda 1}\lambda_1(t) + \frac{2}{N_0}[y - \lambda_1 - q(z_1)]\left[D_{1\lambda} + D_{1\lambda z}q'(z_1)\right] - a_{21\lambda}\frac{\omega_{2\lambda}}{\omega_{1\lambda}}\left(\frac{D_{1\lambda}}{D_{2\lambda}}\right)^{3/2} *$$
$$*(\lambda_1 - \lambda_2)\exp\left\{-\frac{(\lambda_1 - \lambda_2)^2}{2D_{2\lambda}}\right\} - a_{31\lambda}\frac{\omega_{3\lambda}}{\omega_{1\lambda}}\left(\frac{D_{1\lambda}}{D_{3\lambda}}\right)^{3/2} *(\lambda_1 - \lambda_3)\exp\left\{-\frac{(\lambda_1 - \lambda_3)^2}{2D_{3\lambda}}\right\}; \quad (4)$$

Также решена задача синтеза фильтра, когда сигнал и помеха представляются непрерывными марковскими процессами без использования дискретных состояний для описания процесса изменения функции сигнала во времени, получена система выражений (5 – 9) определяющая схему алгоритма нелинейной фильтрации непрерывных марковских процессов в нестационарном режиме.

$$\frac{\partial\lambda}{\partial t} = -k_1\lambda + \frac{2}{N_0}(y - \lambda - q(z))(D_\lambda + D_{\lambda z}q'(z)) \quad (5)$$

$$\frac{\partial z}{\partial t} = -k_2 z + \frac{2}{N_0}(y - \lambda - q(z))(D_{\lambda z} + D_z q'(z)) \quad (6)$$

$$\frac{\partial D_\lambda}{\partial t} = \frac{1}{2}N_\lambda - 2k_1 D_\lambda - \frac{2}{N_0}(D_\lambda^2 + 2D_\lambda D_{\lambda z}q'(z) + D_{\lambda z}^2(q'^2(z) - (y - \lambda - q(z))q''(z)) \quad (7)$$

$$\frac{\partial D_z}{\partial t} = \frac{1}{2}N_z - 2k_2 D_z - \frac{2}{N_0}[D_z^2(q'^2(z) - (y - \lambda - q(z))q''(z)) + 2D_z D_{\lambda z}q'(z) + D_{\lambda z}^2] \quad (8)$$

$$\frac{\partial D_{\lambda z}}{\partial t} = \frac{1}{2}N_{\lambda z} - D_{\lambda z}(k_1 + k_2) - \frac{2}{N_0}[D_\lambda(D_{\lambda z} + D_z q'(z)) + \quad (9)$$
$$+ D_{\lambda z}(D_z(q'^2(z) - (y - \lambda - q(z))q''(z)) + D_{\lambda z}q'(z)]$$

В **четвертой главе** проведены экспериментальные исследования цифровых алгоритмов обработки сигнала ПЭМИ во временной и спектральной области на основе алгоритмов синтезированных в теоретических разделах диссертации. Для проведения цифрового моделирования были записаны информативные сигналы при помощи токосъемника ТИ2-3 с одного информационного провода, с двух информационных проводов, с неэкранированного и экранированного кабеля. С помощью БПФ был найден спектр записанных сигналов всех клавиши (рисунок 3). Исследования в спектральной области позволили оценить возможность обнаружения сигнала ПЭМИ клавиатуры интерфейса USB без учета наличия информационных пакетов данных в сигнале. Для исследования потенциальных возможностей обнаружения информативной составляющей сигнала ПЭМИ клавиатуры USB был проведен эксперимент в режиме широкополосного приема сигнала. На основании полученных графиков нормированных ВКФ от отношения С/Ш (рисунок 4) производился расчет дальности обнаружения информативного сигнала.

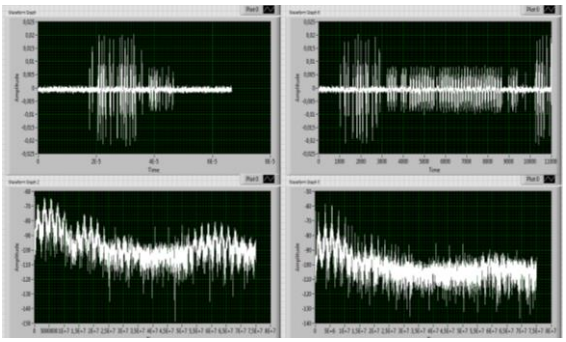

Рис. 3 – Сигналы ПЭМИ опроса и ответа и их спектры.

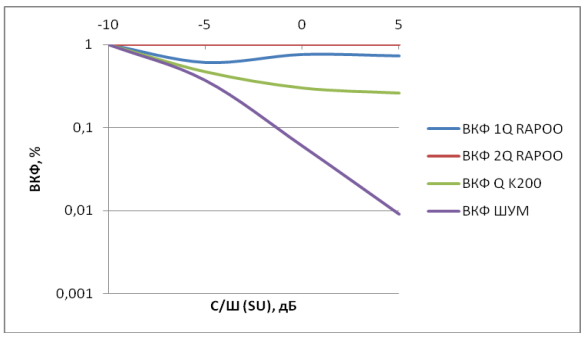

Рис. 4 – Графики зависимости НВКФ от отношения С/Ш для S_U помехи.

Были оценены потенциальные возможности обнаружения сигнала ПЭМИ клавиатуры интерфейса USB. Для этого была рассчитана дальность до точки в пространстве, при которой отношение мощности сигнала к мощности суммы внешних и внутренних шумов приемника снизиться до критического уровня, определенного в эксперименте 1: до -5 дБ для БГШ и S_U помехи Джонсона, до -10 дБ для S_B помехи Джонсона, до 0 дБ для S_L помехи Джонсона для стандартизованных параметров распределения (γ=0, η=1).

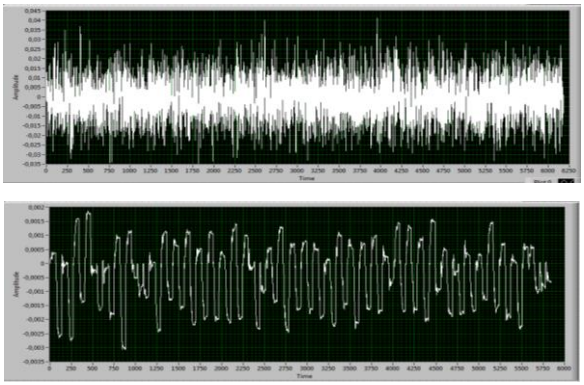

Рис. 5 – Сигнал ПЭМИ с данными о нажатии клавиши «Q» в смеси с БГШ и восстановленный сигнал.

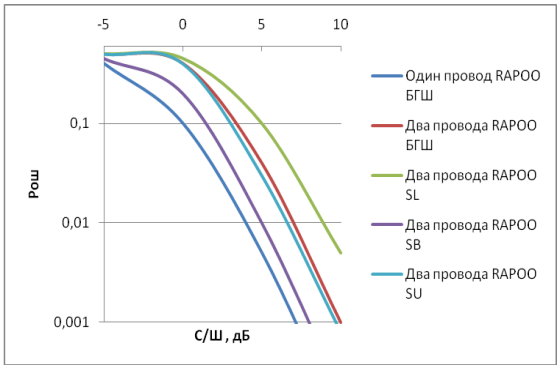

Рис. 6 – График зависимости $P_{ош}$ правильного восстановления данных о нажатии клавиши от отношения С/Ш.

В эксперименте 2 исследовались возможности обнаружения сигнала во временной области с помощью коррелятора, при этом рассчитывается ВКФ между смесью сигнала и помех и опорным сигналом. В результате цифрового эксперимента 3, в котором оценивалось значение максимума взаимной корреляционной функции сигнала ПЭМИ, прошедшего через нелинейный фильтр марковских процессов, и опорного сигнала, в зависимости от отношения С/Ш на входе приемного устройства для БГШ и одного из трех видов помех Джонсона, было показано, что использование разработанного алгоритма нелинейной фильтрации марковских процессов позволяет увеличить критическое значение отношения С/Ш, при котором возможно обнаружение сигнала ПЭМИ клавиатуры USB для всех видов помех.

В эксперименте 4 и 5 исследовались возможности восстановления импульсной последовательности, содержащей данные о нажатии клавиши для различных типов принимаемого и опорного сигналов и помех как с известным временем прихода первого импульса, так и системой синхронизации с использованием разработанного алгоритма оптимального приема по критерию минимума среднего риска, результат работы которого представлен на рисунке 5. В результате эксперимента были получены зависимости вероятности ошибки правильного восстановления данных о нажатии клавиши от отношения С/Ш для различных помех (рисунок 6), показывающие потенциальные возможности восстановления реального сигнала ПЭМИ проводной USB клавиатуры.

В **пятой главе** проводится детерминированный факторный анализ параметров системы перехвата информации из ПЭМИ USB клавиатуры. Установлено влияние априорных сведений о сигнале и помехе в системе обнаружения и восстановления информации по каналам побочного электромагнитного излучения USB клавиатуры на выбор наиболее эффективного метода обработки сигнала.

Заключение содержит формулировки основных научных и практических результатов диссертационной работы.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

В диссертационной работе дано новое решение актуальной научно-технической задачи по разработке эффективных алгоритмов обнаружения и восстановления информации из сигналов ПЭМИ клавиатуры USB интерфейса при действии гауссовских и негауссовских S_L, S_B и S_U помех Джонсона в условиях различной априорной неопределенности, основанных на перспективных методах обработки сигнала, и, как следствие, повышению информационной безопасности и эффективности радиопротиводействия перехвату утечки информации. Основные научные и практические результаты исследований сводятся к следующему:

1. Разработаны алгоритм совместной нелинейной фильтрации непрерывных и дискретного марковских процессов и упрощенный алгоритм нелинейной фильтрации двумерных непрерывных марковских процессов, описывающих сигнал побочного электромагнитного излучения клавиатуры ПЭВМ интерфейса USB и помеху, с нормальным распределением плотности вероятности или распределением Джонсона для работы в нестационарном режиме. При этом использование алгоритма совместной нелинейной фильтрации непрерывных и дискретного марковских процессов позволяет повысить качество фильтрации сигналов ПЭМИ для всех видов помех, однако является труднореализуемым на практике по сравнению с алгоритмом двумерной фильтрации.

2. Использование разработанного алгоритма нелинейной фильтрации марковских процессов позволяет увеличить критическое значение отношения С/Ш, при котором возможно обнаружение сигнала ПЭМИ клавиатуры USB для всех видов помех на 2 дБ. Использование разработанного алгоритма нелинейной фильтрации марковских процессов для гауссовских помех позволяет существенно увеличить качество обнаружения сигнала ПЭМИ для отношений С/Ш больших -5 дБ; для негауссовских помех – для отношений С/Ш больших -7 дБ.

3. Разработанные алгоритмы оптимального приема по критерию минимума среднего риска позволяют восстанавливать данные, содержащиеся в побочном электромагнитном излучении клавиатуры интерфейса USB. Использование разработанного алгоритма позволяет восстанавливать данные снятые с дифференциальной пары с известной клавиатуры до критического значения отношения С/Ш -2 дБ при действии БГШ, до критического значения отношения С/Ш 2 дБ для неизвестной клавиатуры, и до критического значения отношения С/Ш 2 дБ при действии S_L помехи Джонсона.

4. Теоретический анализ оптимального алгоритма по критерию минимума среднего риска доказал, что использование помех, имеющих законы распределения Джонсона приводит к проигрышу в мощности помехи, который может достичь 50 дБ, но может принимать значения в несколько децибел в зависимости от значений параметров распределений Джонсона и от степени коррелированности помехи. В частности, проигрыш в маскирующем действии коррелированных помех Джонсона меньше некоррелированных. Так, например, проигрыш S_L помехи по сравнению с гауссовой при стандартизированных параметрах распределения (η=1 и γ=0) составляет 18,39дБ для некоррелированной помехи и 15,38дБ для коррелированной.

5. В результате проведения эксперимента были оценены потенциальные возможности обнаружения сигнала ПЭМИ клавиатуры интерфейса USB в идеальных условиях без воздействия внешнего шума и реальные возможности обнаружения сигнала ПЭМИ в условиях естественного шума БГШ и искусственных помех Джонсона. При этом дальность обнаружения в идеальном случае составляет около 3 м от экранированного кабеля и не превышает 50 см от экранированного кабеля для БГШ и S_U, S_L и S_B помехи Джонсона в реальных условиях.

6. На основании детерминированного факторного анализа установлена степень влияния различных параметров системы перехвата на качество восстановления информации. Исследование показало, что достижение максимально эффективного радиопротиводействия осуществляется выбором маскирующей помехи. При этом наибольший маскирующий эффект помех Джонсона достигается при γ равном 0 и максимальном η.

7. Применение разработанных алгоритмов оптимального приема и алгоритмов нелинейной фильтрации возможно в различных радиолокационных, телекоммуникационных, финансовых системах, а также в системах обработки изображений.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых научных изданиях, рекомендованных ВАК Минобрнауки России опубликовано 3 статьи:

1. Астрецов Д.В. Оптимальный прием бинарного сообщения, основанный на методе совместной нелинейной фильтрации непрерывных и дискретного марковских процессов / Д.В. Астрецов, Р.И. Соколов // Научно-технический вестник Поволжья. – Казань, 2014. – №4. – С. 41-44.
2. Астрецов Д.В. Применение нелинейной марковской фильтрации в приёмных устройствах радиолокационных и телекоммуникационных систем / Д.В. Астрецов, Р.И. Соколов, Д.А. Долматов // Наука и бизнес: пути развития. – Москва, 2015. – №6. – С. 33-38.
3. Соколов Р.И. Фильтрация случайной составляющей цены актива методом нелинейной марковской фильтрации / Р.И. Соколов // Вестник УрФУ: Экономика и управление. – Екатеринбург, 2015. – Том 14. – №1. – С. 145-161.

Публикации в трудах конференций, реферируемых в базе данных «SCOPUS»:

4. Sokolov R.I. Research of optimal pulse signal reception quality by mean risk minimum criterion with action of Gaussian and non-Gaussian noise / R.I. Sokolov, R.R. Abdullin // Source of the Document International Conference on Computational Techniques in Information and Communication Technologies, ICCTICT 2016. – New Delhi, India, 2016. – P. 97-100.
5. Sokolov R.I. Synthesis of ultra-wideband signals receiver algorithm based on Markov theory of nonlinear filtering / R.I. Sokolov, R.R. Abdullin // Source of the Document Asia-Pacific Microwave Conference Proceedings (APMC 2015). – Nanjing, China, 2015. [Электронный ресурс], режим доступа: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7411681.
6. Astretsov D.V. Quasioptimal nonlinear filtering of binar signals in Johnson noise condition / D.V. Astretsov, R.I. Sokolov // Source of the Document 24th International Crimean Conference Microwave and Telecommunication Technology (CriMiCo 2014). – Sevastopol, Russia, 2014. – P. 427-428.
7. Sokolov R.I. Quasi-optimal nonlinear Markov receiver in airborne radar based on waveguide-slotted antenna/ R.I. Sokolov, R.R. Abdullin // Proceedings of the 2015 IEEE 4th Asia-Pacific Conference on Antennas and Propagation, APCAP 2015. – Bali Island, Indonesia, 2015. – P. 77-78.

Публикации в реферируемых изданиях, учитываемых в базе данных РИНЦ и в трудах всероссийских и международных конференциях:

8. Астрецов Д.В. Анализ потенциальной помехоустойчивости выделения бинарного сообщения при действии гауссовских и негауссовских помех / Д.В. Астрецов, Ю.А. Нифонтов, Р.И. Соколов // XI Международная научно-техническая конференция “Физика и технические приложения волновых процессов”: сборник трудов конференции. – Екатеринбург: Изд. УрФУ, 2012. – С. 147–149.

9. Астрецов Д.В. Потенциальная помехоустойчивость выделения бинарного сообщения при действии негауссовских помех / Д.В. Астрецов, Ю.А. Нифонтов, Р.И. Соколов // XI Всероссийская научно-техническая конференция молодых ученых “Безопасность информационного пространства”: Сборник статей по материалам конференции. – Тюмень: Изд. ТГУ, 2012. – С. 215–223.

10. Астрецов Д.В. Анализ моделирования выделения бинарного сигнала при действии помех Джонсона различными оптимальными приемниками / Д.В. Астрецов, Ю.А. Нифонтов, Р.И. Соколов // XVII Всероссийская научно-техническая Интернет-конференция молодых ученых "Информационные технологии и электроника": Материалы конференции. – Екатеринбург, 2012. [Электронный ресурс], режим доступа: http://webconf.rtf.urfu.ru/mod/forum/ discuss.php?d=998.

11. Астрецов Д.В. Ситнез алгоритмов нелинейной фильтрации сигналов ПЭМИ при действии гауссовых и негауссовых помех. / Д.В. Астрецов, Р.И. Соколов // XII Всероссийская научно-техническая конференция молодых ученых “Безопасность информационного пространства”: Сборник статей по материалам конференции. – Екатеринбург: Изд. УрФУ, 2013. – С. 44 –48.

12. Астрецов Д.В. Опыт применения комплекса беспроводной связи в реализации приемников ПЭМИ / Д.В. Астрецов, Р.И. Соколов // Международная научно-практическая конференция “Перспективы развития науки и образования”: Сборник научных трудов. – Тамбов: Изд. ТРОО “Бизнес-Наука-Общество”, 2014. – Т.4. – С. 149-150.

13. Астрецов Д.В. Эффективность оптимального приемника нелинейной фильтрации при действии негауссовских помех / Д.В. Астрецов, Р.И. Соколов // XV Международная научно-практическая конференция “Современные информационные и электронные технологии”: Сборник трудов конференции. – Украина, Одесса: Изд. “Политехпериодика”, 2014. – Т.1. – С. 203-204.

14. Астрецов Д.В. Нелинейная марковская фильтрация бинарного сообщения при действии негауссовских помех / Д.В. Астрецов, Р.И. Соколов // XII Международная научно-техническая конференция “Актуальные проблемы электронного приборостроения-2014”: Сборник трудов конференции. – Новосибирск: Изд. НГТУ, 2014. – С. 159-161.

15. Соколов Р.И. Детерминированный факторный анализ параметров системы выделения конфиденциальной информации / Р.И. Соколов // Международная конференция молодых ученых “Информационные технологии, телекоммуникации и системы управления”: Сборник трудов конференции. – Екатеринбург: Изд. УрФУ, 2014. [Электронный ресурс], режим доступа: http://lib.urfu.ru/course/view.php?id=148.

16. Кобяков В.Ю. Возможности восстановления информационных сигналов ПЭМИ клавиатуры USB интерфейса / В.Ю. Кобяков, Р.И. Соколов // XIV Всероссийская научно-техническая

конференция молодых ученых “Безопасность информационного пространства”: Сборник статей конференции. – Тюмень: изд. ТГУ, 2015. – С. 156-163.
17. Астрецов Д.В. Потенциальные возможности обнаружения спектральных составляющих ПЭМИ сигнала клавиатуры USB интерфейса / Д.В. Астрецов, В.Ю. Кобяков, Р.И. Соколов // II Международная конференция молодых ученых “Информационные технологии, телекоммуникации и системы управления”: Сборник статей конференции. – Екатеринбург: Изд. УрФУ, 2015. – С.152-160.