ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
СПбГУТ))) Март 2017 Том 5 № 1 ISSN 2307-1303 http://www.itt.sut.ru
TELECOM IT
March 2017 Vol. 5 Iss. 1 ISSN 2307-1303 http://www.itt.sut.ru

АНАЛИТИЧЕСКИЙ ОБЗОР ПО ИССЛЕДОВАНИЯМ ВЛИЯНИЯ ПРЕДНАМЕРЕННОГО ЭЛЕКТРОМАГНИТНОГО ВОЗДЕЙСТВИЯ НА БЕСПРОВОДНЫЕ СЕТИ

Л. Ч. Хоанг[1], Р. В. Киричек[1*]

[1] СПбГУТ, Санкт-Петербург, 193232, Российская Федерация
* Адрес для переписки: kirichek@sut.ru

Аннотация
Интернет вещей может быть привлекательным с использованием любой технологии, совместимой с Интернетом, такие как Wi-Fi, беспроводные сенсорные сети, сети с малым задержкам и т. д. Эти технологии хорошо установлены и способны полностью функционировать для интернет-коммуникаций и, как таковые, подходят для того, чтобы стать основой Интернета Вещей. Однако, несмотря на все преимущества беспроводных технологий в настоящее время для них существует ряд потенциальных уязвимостей, имеющих естественный и искусственный характер. При этом необходимо учесть, что сегодня в мире существует реальная угроза воздействия на беспроводные сети различных деструктивных электромагнитных воздействий, одним из которых является преднамеренное электромагнитное воздействие (ПД ЭМВ). **Предмет исследования.** Статья посвящена исследованию влияний преднамеренного электромагнитного воздействия на беспроводные сети. **Метод.** В качестве метода исследования проводится аналитический обзор существующих подходов по исследованиям влияния преднамеренного электромагнитного воздействия на беспроводные сети. **Основной результат.** В рамках данной работы было показано, что, несмотря на многообразие аналогичных исследований, проведенных как в России, так и за рубежом, рассматриваемая проблема не была решена в полной мере. **Практическая значимость.** Отмечено, что для качественного анализа рассматриваемой в работе проблемы имеется необходимость исследования полного комплекса механизмов деструктивного воздействия, а так же проведение испытаний устойчивости беспроводных сетей в заданных условиях с использованием общепризнанных методик их диагностики.

Ключевые слова
сети связи, беспроводная технология, преднамеренные электромагнитные воздействия (IEMI), защита, влияние.

Информация о статье
УДК 621.39
Язык статьи – русский.
Поступила в редакцию 15.02.17, принята к печати 28.02.17.

Ссылка для цитирования: Хоанг Л. Ч., Киричек Р. В. Аналитический обзор по исследованиям влияния преднамеренного электромагнитного воздействия на беспроводные сети // Информационные технологии и телекоммуникации. 2017. Том 5. № 1. С. 114–125.

OPEN RESEARCH PROBLEMS AND POSSIBLE APPLICATIONS FOR TERAHERTZ BAND WIRELESS NETWORKS

Le Trung Hoang[1], R. Kirichek[1*]

[1] SPbSUT, St. Petersburg, 193232, Russian Federation
* Corresponding author: kirichek@sut.ru

Abstract—The Internet of Things can be attractive using any Internet capable technology, such as Wi-Fi, wireless sensor networks, Low power and Lossy Networks etc. These technologies are all well established and fully functional for Internet communications and as such are suitable to be a part of the backbone of the Internet of Things. However, despite all the advantages of wireless technologies, there are currently a number of potential vulnerabilities for them that have a natural and artificial nature. At the same time, it is necessary to take into account that today in the world there is a real threat of impact on wireless networks of various destructive electromagnetic influences, one of which is an intentional electromagnetic influence (IEMI). **Research subject.** The article is devoted to the investigation of the effects of intentional electromagnetic interference on wireless networks. **Method.** As a research method conducted an analytical review of existing approaches on the reseach of the impact of intetional electromagnetic inteference on wireless networks. **Core results.** There are many studies both in Russia and abroad devoted to this type of impact affecting on wireless netwoks, but they do not fully solve the problem of protection wireless networks from IEMI. **Practical relevance.** It is noted that for a qualitative analysis of the problem under consideration, it is necessary to investigate the full range of destructive impact mechanisms, as well as conduct stability tests for wireless networks under specified conditions using commonly accepted diagnostic techniques.
Keywords—Communication networks, wireless technology, intentional electromagnetic interference (IEMI), protection, influence.

Article info
Article in Russian.
Received 15.02.17, accepted 28.02.17.

For citation: Hoang Le Trung, Kirichek R.: Analytical review on the research of the influence of intentional electromagnetic interference on wireless networks // Telecom IT. 2017. Vol. 5. Iss. 1. pp. 114–125 (in Russian).

Введение

Современные технологии открывают перед людьми массу возможностей, упрощающих решение повседневных задач. Одной из самых развиваемых, востребованных и перспективных технологий является беспроводная связь. С её помощью появляется возможность объединять различные устройства в группы и обмениваться информацией. При этом все происходит без использования проводов, что позволяет участникам группы свободно перемещаться, оставаясь онлайн.

Несмотря на все преимущества беспроводных сетей в настоящее время для них существует ряд потенциальных уязвимостей, имеющих естественный и искусственный характер. При этом необходимо учесть, что сегодня в мире существует реальная угроза воздействия на беспроводные сети различных деструктивных электромагнитных воздействий, одним из которых является преднамеренное электромагнитное воздействие (ПД ЭМВ).

Преднамеренные электромагнитные воздействия на объекты и средства информатизации могут осуществляться по эфиру, цепям электропитания, линям связи и металлоконструкциям с помощью генераторов сверхкоротких электромагнитных импульсов (СК ЭМИ).

Для этих воздействий свойственны:

- возможность проведения атак из-за пределов контролируемых зон;
- отсутствие явных демаскирующих признаков;
- маскировка под действие электромагнитных помех;
- отсутствие в действующем законодательстве юридической основы, предусматривающей административную и уголовную ответственность за проведение электромагнитных атак и др.

Данные воздействия являются наиболее критичными для средств информатизации, функционирующих в реальном времени, таких, как: средства связи и телекоммуникации, автоматизированные системы управления технологическими процессами, элементы систем физической защиты объектов и др.

Последствия нарушения функционирования этих систем соизмеримы с последствиями проведения прямых террористических атак. Применяя подходы и термины в области безопасности информационных технологий, изложенные в международном стандарте ИСО/МЭК 15408-1 (Общие критерии)[1], угрозу ПД ЭМВ на информационную систему можно охарактеризовать как угрозу злоумышленных действий, направленных на уничтожение, искажение и блокирование информации. Поэтому деятельность, направленная на обеспечение защиты средств информатизации от данной угрозы, является актуальной.

Основными направлениями деятельности в этой предметной области, проводимой в России и за рубежом, являются:

- исследование изменения характеристик СК ЭМИ при прохождении через конструктивные элементы объектов;
- исследование механизмов деструктивных воздействий на средства информатизации;
- разработка методов и средств защиты от данной угрозы;
- создание нормативной базы в виде системы целевых стандартов.

В данной работе проводим аналитический обзор по исследованию влияния ПД ЭМВ на беспроводные сети, доступных автору.

Электромагнитный терроризм. Преднамеренные электромагнитные воздействия

Первое широкое обсуждение проблемы «электромагнитного терроризма» можно отнести к 1996 г. [1, 2]. Под воздействием средства электромагнитного терроризма понимается преднамеренное мощное электромагнитное воздействие, в результате которого происходит сбой в работе электронных средств, а также физическое разрушение их элементов; искажение, уничтожение или блокирование информации[2].

[1] ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

[2] ГОСТ Р 51275-2007. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М.: Стандартинформ. 2007. 10 с.

Требования к излучателям ПД ЭМВ и рекомендации по определению их метрологических характеристик обоснованы в [3]. Для расчета антенно-фидерных систем автором применен простой аналитический способ расчета полей от бегущих волн тока, распространяющихся по тонким криволинейным проводам, расположенным на электродах исследуемых полеобразующих систем. По результатам проведенных экспериментальных исследований воздействия СЭТ на персональные компьютеры и систему контроля доступа видно, что амплитуда воздействующего импульса СЭТ, приводящая к зависанию персонального компьютера, в среднем составляет 3 кВ/м, а для сбоя в работе системы контроля доступом достаточным является 7 кВ/м.

Одним, из ПД ЭМВ является новое эффективное сверхкоротко-импульсное электромагнитное излучение (СКИ ЭМИ). СК ЭМИ являются разновидностью сверхширокополосных сигналов (*Ultra Wide Band*). По определению Федеральной комиссии связи США (FCC) к ним относятся все излучения, у которых ширина спектральной полосы по уровню – 10 дБ составляет, по крайней мере, 25 % от значения центральной частоты. К источникам с такими параметрами относятся, в частности, излучатели СК ЭМИ, формирующие импульсы, представляющие собой несколько полупериодов высокой частоты.

Особенностью СК ЭМИ является их малая длительность (от десятков-сотен пикосекунд до единиц наносекунд для первых полупериодов импульсов по уровню 0,5 от амплитуды), соизмеримая с длительностью рабочих сигналов электронной аппаратуры и сетей передачи данных. Основная спектральная плотность находится в полосе частот от сотен мегагерц до единиц гигагерц. Высокая скважность обеспечивает большие значения импульсных напряженностей при низких уровнях средней мощности (< 1 Дж) и энергопотребления источника.

Для исследования последствий воздействия преднамеренных электромагнитных импульсов на беспроводные сети используют лабораторные генераторы. В лабораторных генераторах СК ЭМИ на выходе генератора формируются периодически повторяющиеся видеоимпульсы положительной или отрицательной полярности.

В результате воздействия направленного излучения на беспроводную сеть происходит искажение и блокирование информации, передающейся в сети. Это происходит в результате того, что на приемном тракте помимо полезных сигналов происходит прием сверхкоротких импульсных помех, которые в силу аддитивной природы изменяют исходную форму полезных сигналов. В результате декодированию импульсов происходит отбрасывание некорректных кадров. Таким образом насущно необходимо разработать алгоритмы и методы гарантированной передачи данных в беспроводной сети, на которую воздействует электромагнитное поле, сформированное СШП генератором.

Очевидным, что на сегодняшний день электромагнитное оружие на основе генераторов сверхширокополосных электромагнитных импульсов является одним из главных видов оружия XXI в. и представляет наибольшую опасность для электронной инфраструктуры объектов информатизации, каковыми являются, в частности, беспроводные сети.

Международная деятельность по исследованию преднамеренных электромагнитных воздействий

На международном уровне ежегодно проводятся конференции и симпозиумы по данной проблеме. Наиболее активными участниками являются: США, Германия, Швеция, Япония, Китай, Россия.

Органам, осуществляющими развитие направлений стандартизации в данной области, являются непосредственно МЭК (IEC) и МСЭ-Т (ITU-T).

IEC SC77C дальше всех других продвинулись в направлении стандартизации сферы защиты от ПД ЭМВ.

Активная деятельность ведется по разработке международных стандартов в рамках подкомитета 77С МЭК (председатель Уильям Радаски). В настоящий момент фокус стандартов SC77C смещен в сторону защиты от ЭМИ высокой мощности (*High Power Electromagnetic* – HPEM). Разработаны 19 документов: 14 международных стандартов и 5 технических докладов МЭК в которых изложены: обзор данного вида ЭМИ, методология измерений, параметры нагружения.

За последнее время дополнительно разработаны стандарты (табл. 1) по методам защиты распределенных системы инфраструктуры от ПД ЭМВ и методам оценки устойчивости систем к HPEM воздействиям [4].

Таблица 1.

Стандарты МЭК 2009 г.

IEC/TR 61000-4-35:2009	Электромагнитная совместимость (EMC). Часть 4–35. Методы испытаний и измерений. Краткое руководство по устройствам, моделирующим HPEM
IEC/TS 61000-5-8:2009	Электромагнитная совместимость (EMC). Часть 5–8. Руководства по монтажу и подавлению помех. Методы защиты от HEMP для распределенной инфраструктуры
IEC/TS 61000-5-9:2009	Электромагнитная совместимость (EMC). Часть 5–9. Руководства по монтажу и подавлению помех. Оценки магнитной восприимчивости на уровне системы для HEMP и HPEM

В 2005 году МСЭ-Т исследовательской группой № 5 (SG5) были начаты обсуждения рекомендаций, связанных исследованием влияния ПД ЭМВ на телекоммуникационную аппаратуру. До 2012 года запланировано выпустить рекомендации, в которых будут приведены значения напряженности поля на различных расстояниях, и т.д. для того, чтобы позволить оценить степень риска, и предложены соответствующие меры противодействия электромагнитным атакам [5]. Одной из последних является рекомендация K.81 «HPEM immunity guide for telecommunication systems», посвящённая испытаниям на устойчивость телекоммуникационной аппаратуры и центров обработки данных к воздействию ПД ЭМВ.

Аналитический обзор по исследованиям влияния преднамеренного электромагнитного воздействия на беспроводные сети

Обзор публикаций показывает, что исследуемая проблема малоизучена ввиду ряд факторов. Во-первых, исследованием данной проблемы занимается узкий круг специалистов, которые не достаточно взаимодействуют между со-

бой (возможно, это вызвано закрытостью значительной части проводимых исследований). Во-вторых, большая часть работ в этой области посвящена исследованиям влияния ПД ЭМВ непосредственно на телекоммуникационную аппаратуру, а воздействие на беспроводные сети как отдельная проблема не рассматривается. В-третьих, в России и за рубежом уделяют большое внимание постановке натурных испытаний и получению видимых эффектов, однако при этом авторы неглубоко вникают в механизмы обнаружения влияния ПД ЭМВ на беспроводные сети, а также в механизмы защиты беспроводных сетей от этих явлений. Наблюдается стремление к количественным результатам, но не к качественному пониманию сути процессов.

В данной работе будет рассматриваться во всем подробнее, исходя из материалов исследований влияния ПД ЭМВ на беспроводные сети, доступных автору.

За рубежом идеологом первого направления исследований является известный американский ученый Ira Kohlberg. Обзор его публикаций за последние годы свидетельствует о развитии и совершенствовании расчетных методов для оценки уязвимости систем информационной инфраструктуры. В большинстве рассмотренных статей показано, что наибольшую опасность представляют преднамеренные электромагнитные воздействия, амплитудно-временные характеристики которых аналогичны характеристикам рабочих сигналов современных электронных систем.

Но именно по изучению восприимчивости и уязвимости беспроводных сетей к преднамеренным электромагнитным воздействиям только обратили специалистам, а также ученным в последние 5 лет.

В [6] представлены результаты анализа особенности влияния ПД ЭМВ на процесс передачи данных в беспроводной сети. В рамках данной работы, автор рассмотрел два различных вида помехи. Первая представляет собой импульс постоянной амплитуды с частотой на 500 кГц выше частоты полезного сигнала (2,431 ГГц). Вторая помеха это двойной экспоненциальной импульс, который сдвигается по частоте полезного сигнала. Эти помехи только осуществляют по беспроводной линии связи, а не имеет свойства наносить ущерб на компоненты сети. Пример формы полезного сигнала и помехи представлен на рис. 1.

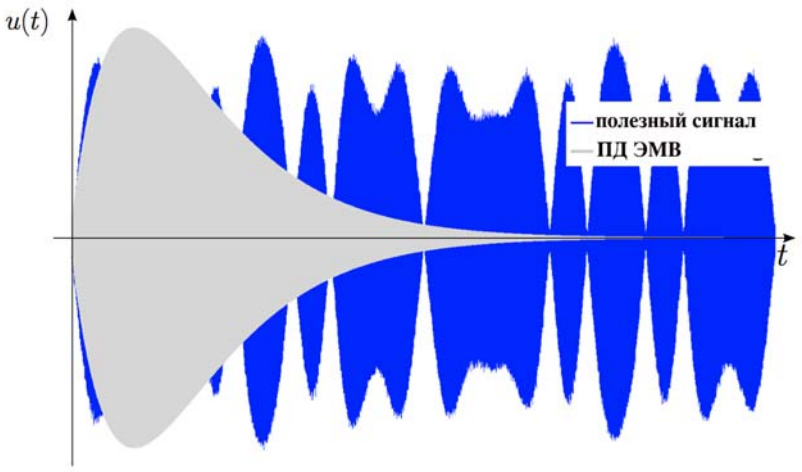

Рис. 1. Пример формы полезного сигнала и сигнал помехи

В результате показано, что влияние ПД ЭМВ на беспроводные линии связи оказывается соизмеримость длительности действующих импульсов с длительностью информационного сигнала на приеме (рис. 2).

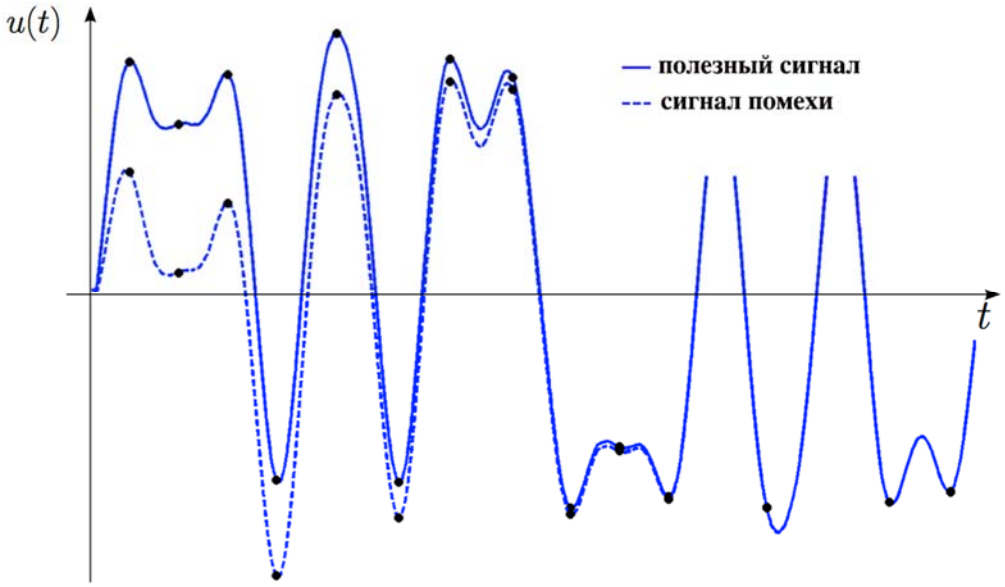

Рис. 2. Особенность влияния ПД ЭМВ на беспроводные линии связи

Автор в [7] предложил метод для оценки уровней защиты беспроводных телекоммуникационных инфраструктур от ПД ЭМВ. Требуемые уровни защиты определяются путем анализа восприимчивости жертвы и угрозы, связанные с конкретными сценариями атаки беспроводных сетей по ПД ЭМВ.

Данный метод применяется для разработки стратегии защиты базовой станции от повреждения из-за помех в полосе с использованием радиочастотного ограничителя (рис. 3.).

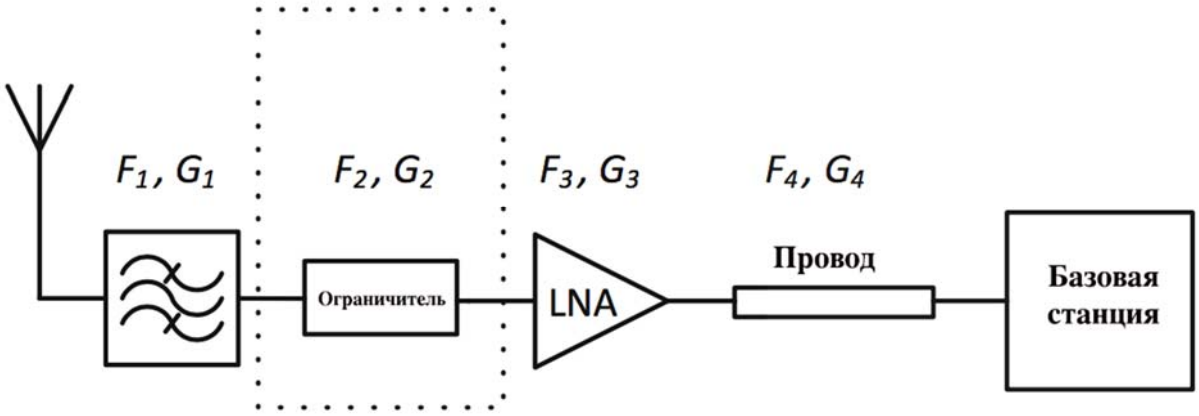

Рис. 3. Защита базовой станции с применением радиочастотного ограничителя

Коэффициент шума F вычисляется как

$$F = \frac{SNR_{in}}{SNR_{out}},$$

где SNR_{in} – это входное отношение сигнал/шум (дБ), SNR_{out} – это выходное отношение сигнал/шум (дБ).

Общий коэффициент шумов F_{total} зависит коэффициентов шума F_i и передачи G_j отдельных компонентов будет равен

$$F_{total} = F_1 + \frac{F_2 - 1}{G_1} + \frac{F_3 - 1}{G_1 G_2} + \frac{F_4 - 1}{G_1 G_2 G_3}.$$

Типичные значения коэффициентов шумов и передачи приведены в табл. 2.

Таблица 2.

Типичные значения коэффициентов шумов и передачи

Компонент	**Коэффициент шумов (дБ)**	**Коэффициент передачи (дБ)**
1. Фильтр	1	-1
2. Ограничитель	1	-1
3. LNA (Low-Noise Amplifier)	2	20
4. Кабель	4	-4

Автор в данной работе доказано, что деградация коэффициента шумов линейно зависит от вносимых потери ограничителя (рис. 4.).

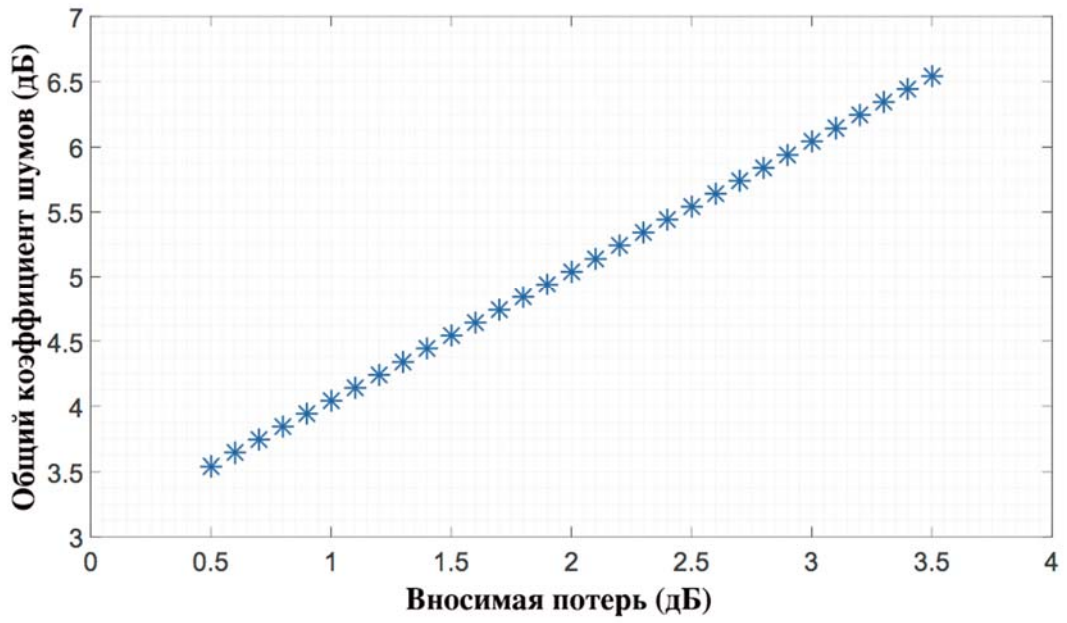

Рис. 4. Зависимость коэффициента шумов от вносимых потери ограничителя

В работе [8] рассмотрен новый подход по локализации источника ПД ЭМВ. Предложенный автором метод оценки разности времён прихода сигналов (*Time Difference of Arrival*, TDoA) позволяет локализовать местоположения источника

воздействия. Данный алгоритм основан на измерении разностей времён прихода сигналов на различные устройства. Зная положение устройства в сети можно оценить местоположение источника помеха путем анализа зависимости между разницы во времени и расстояния, распространяемых электромагнитные волны.

Автор предложил, что координаты источника воздействия и *i*-го сенсора в декартовой системе следовательно: $[x_S, y_S, z_S]$ и $[x_i, y_i, z_i]$. В качестве примера было доказано, что добавляя еще два устройства и таким образом еще два уравнения, полученная система трех уравнений стала решаемой. Однако, так как уравнения нелинейны, больше чем одно решение существует. Для многих практических ситуаций это незначительный недостаток, поскольку неправильные решения могут быть определены. Автор в [9] показал, что в последнем варианте, когда атака ПД ЭМВ поступает на пять соединений и более то система уравнения решается и она является линейной. Таким образом, чем больше количество соединений, на которые поступает воздействие помехи, тем более вероятность его локализовать.

Среди публикаций отечественных специалистов, занимающих методом и средством оценки влияния ПД ЭМВ на системы радиосвязи, можно отметить следующие статьи [10, 11, 12, 13, 14]. Существует достаточно много работ, посвященных влияния данного вида воздействия на различные виды сетей связи. Проводились исследования для выявления устойчивости системы электросвязи к преднамеренным электромагнитным воздействиям [15], а также разработки новых стандартов в противодействии электромагнитной атаки [16].

В своих работах [10, 11], автор рассмотрел системы радиосвязи как узкополосные, широкополосные и сверхширокополосные системы радиосвязи, а сверхкороткий электромагнитный импульс (СК ЭМИ) как один из наиболее эффективных ПД ЭМВ. Основной особенности воздействия сверхкороткого электромагнитного импульса является то , что сформированный импульсом спектр перекрывает спектр широкополосного и сравним со спектром сверхширокополосного сигнала. Исходя из специфики сверхкороткого электромагнитного импульса, для оценки потенциального влияния необходим подход, анализирующий перекрытие областей спектра воздействующего импульса и спектра сигнала в точке приема. Потенциально влияние может быть оказано при перекрытии большей площади спектра полезного сигнала.

В качестве примера автором приведены изображения спектров сверхширокополосного, широкополосного, узкополосного сигналов связи и сверхкороткого электромагнитного импульса (рис. 5).

Сверхкороткий электромагнитный импульс, ввиду своей широкополосности и относительно постоянной спектральной плотности мощности, может оказывать различное влияние на разные системы связи при одних и тех же энергетических характеристиках. С учетом сопоставления спектров можно сделать вывод о следующих степенях влияния сверхкороткого электромагнитного импульса на средства связи, в порядке убывания:

- Сверхширокополосные средства связи.
- Широкополосные средства связи.
- Узкополосные средства связи.

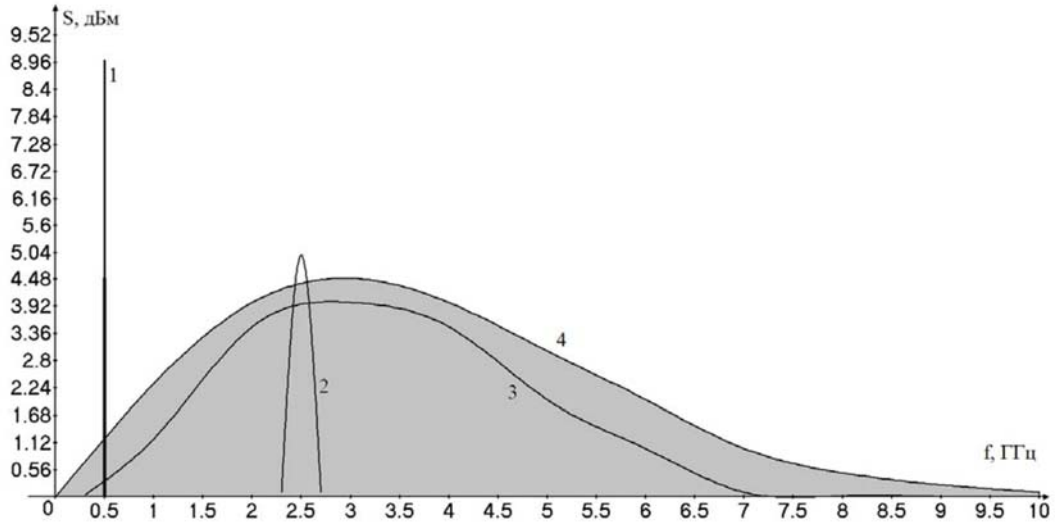

Рис. 5. Условные спектры сигналов:
1 – узкополосная связь, *2* – широкополосная связь, *3* – сверхширокополосная связь,
4 – сверхкороткий электромагнитный импульс

А также были классифицированы механизмы влияния параметров последовательности пакетов СК ЭМИ на средства цифровой радиосвязи (рис. 6).

Рис. 6. Влияния параметров последовательности пакетов СК ЭМИ
на средства цифровой радиосвязи

Из материалов проведенного обзора можно сделать заключение, что хотя уже существует достаточно много исследований за рубежом, посвященных влияния данного вида воздействия на различные виды сетей связи, но они в полной мере не решают проблему защиты беспроводных сетей от ПД ЭМВ. Нужно проводить достаточно полный комплекс исследований механизмов деструктивного воздействия и испытаний устойчивости беспроводных сетей в условиях ПД ЭМВ с использованием общепризнанных методик диагностики сетей. Решение поставленной задачи исключительно экспериментальными методами невозможно. Поэтому при проведении исследований предполагается также использовать расчетно-теоретические методы и имитационное моделирование.

Литература

1. Бакстром М., Баум К., Борисов Р. и др. Электромагнитный терроризм на рубеже тысячелетий. Томск: Изд-во Томск. ун-та. 2002. 206 с.

2. Loborev V. M. The Modern Research Problems // AMEREM Conference. 1996. pp. 29–36.

3. Михеев О. В., Сахаров К. Ю., Соколов А. А., Туркин В. А. Эталонные и испытательные источники электромагнитных импульсов // Измерительная техника. 2005. № 11. С. 55–57.

4. Radasky W. A. Protection of Commercial Installations from the High-Frequency Electromagnetic Threats of HEMP and IEMI using IEC Standards // Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC). 2010. pp. 758–761.

5. Tominaga T., Kobayashi R., Sekiguchi H., Seto S. Standardization Related to Electromagnetic Security // NTT Technical Review. 2008. Vol. 6 No. 10. pp. 1–7.

6. Marcin M., Hamann D., Garbe H. Analysis of IEMI Induced Distortion on Wireless Digital Data Transmission Links // Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC). 2015. pp. 1–4.

7. Van de Beek S. et al. Protection Strategy against IEMI for Wireless Communication Infrastructures // International Symposium on Electromagnetic Compatibility (EMC Europe). 2016. pp. 455–460.

8. Stojilović M. et al. TDoA-based Localisation of Radiated IEMI Sources // International Symposium on Electromagnetic Compatibility (EMC Europe). 2014. pp. 1263–1268.

9. Xu H. A Linear Algorithm based on TDoA Technique for UWB Localization // International Conference on Electric Information and Control Engineering (ICEICE). 2011. pp. 1013–1015.

10. Пименов П. Н. Сравнительный анализ влияния сверхкороткого электромагнитного импульса на узкополосные, широкополосные, сверхширокополосные системы радиосвязи // Технологии ЭМС. 2015. № 1 (52). С. 13–16.

11. Пименов П. Н., Мырова Л. О. Эффективность воздействия сверхкороткого электромагнитного импульса на широкополосные системы радиосвязи // Технологии ЭМС. 2015. № 1 (52). С. 17 –20.

12. Киричёк Р. В. Вероятностная оценка влияния сверхкоротких электромагнитных импульсов на процесс передачи данных в сетях Ethernet // Электросвязь. 2011. № 8. С. 51–54.

13. Данилин С. В., Киричёк Р. В. Вопросы устойчивости активного сетевого оборудования к воздействию сверхкоротких электромагнитных импульсов // Технологии электромагнитной совместимости. 2009. № 1. С. 54–57.

14. Баталов Л. А., Жуковский М. И., Киричёк Р. В., Лазарев Б. Н. Механизмы и последствия преднамеренных электромагнитных воздействий на передачу данных // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 2 (78). С. 103–108.

15. Zhukovsky M., Kirichek R., Larionov S., Chvanov V. Testing of Technical Security Equipment for Stability to Intentional Electromagnetic Interference // 10th International Symposium on Electromagnetic Compatibility (EMC Europe). 2011. pp. 820–823.

16. Kirichek R., Chvanov V. Improvement of Russian Regulatory System on Protection Against Electromagnetic Attacks // 9th International Symposium on Electromagnetic Compatibility joint with the 20th International Wroclaw Symposium on Electromagnetic Compatibility (EMC EUROPE). 2010. pp. 26–29.

References

1. Backström, M., Baum, C., Borisov, R. et al. Electromagnetic Terrorism at the Turn of the Millennium. Tomsk: Izd-vo Tomsk. un-ta. 2002. 206 p.

2. Loborev, V. M. The Modern Research Problems // AMEREM Conference. 1996. pp. 29–36.

3. Sakharov, K., Sokolov, A., Turkin, V., Mikheev, O. Standard and Test Sources of Electromagnetic Pulses // Measurement Techniques. 2005. Vol. 48. Iss. 11. pp. 1120–1124.

4. Radasky, W. A. Protection of Commercial Installations from the High-Frequency Electromagnetic Threats of HEMP and IEMI using IEC Standards // Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC). 2010. pp. 758–761.

5. Tominaga, T., Kobayashi, R., Sekiguchi, H., Seto, S. Standardization Related to Electromagnetic Security // NTT Technical Review. 2008. Vol. 6 No. 10. pp. 1–7.

6. Marcin, M., Hamann, D., Garbe, H. Analysis of IEMI Induced Distortion on Wireless Digital Data Transmission Links // Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC). 2015. pp. 1–4.

7. Van de Beek, S. et al. Protection Strategy against IEMI for Wireless Communication Infrastructures // International Symposium on Electromagnetic Compatibility (EMC Europe). 2016. pp. 455–460.

8. Stojilović, M. et al. TDoA-based Localisation of Radiated IEMI Sources // International Symposium on Electromagnetic Compatibility (EMC Europe). 2014. pp. 1263–1268.

9. Xu, H. A Linear Algorithm based on TDoA Technique for UWB Localization // International Conference on Electric Information and Control Engineering (ICEICE). 2011. pp. 1013–1015.

10. Pimenov, P. A Comparative Analysis of the Influence of Ultra Short Electromagnetic Pulse on Narrowband, Wideband, UWB Radio System // Tekhnologii EMS. 2015. No. 1 (52). pp. 13–16.

11. Pimenov, P., Myrova, L. The Impact of Ultra Short Electromagnetic Pulses for Reducing the Quality of Service Broadband Communication Systems // Tekhnologii EMS. 2015. No. 1 (52). pp. 17–20.

12. Kirichek, R. Probabilistic Estimation of Ultrashort Electromagnetic Pulses' Influence on Data Transmission in Ethernet Networks // Electrosvyaz'. 2011. No. 8. pp. 51–54.

13. Danilin, S., Kirichek, R. Questions of Stability of the Active Network Equipment to Influence of Supershort Electromagnetic Impulses // Tekhnologii EMS. 2009. № 1. С. 54–57.

14. Batalov, L., Zhukovsky, M., Kirichek, R., Lazarev, B. Information Protection against Intentional Electromagnetic Influences // Nauchno-tekhnicheskiy vestnik informatsionnyh tekhnologiy, mekhaniki i optiki. 2012. No. 2 (78). pp. 103–108.

15. Zhukovsky, M., Kirichek, R., Larionov, S., Chvanov, V. Testing of Technical Security Equipment for Stability to Intentional Electromagnetic Interference // 10th International Symposium on Electromagnetic Compatibility (EMC Europe). 2011. pp. 820–823.

16. Kirichek, R., Chvanov, V. Improvement of Russian Regulatory System on Protection Against Electromagnetic Attacks // 9th International Symposium on Electromagnetic Compatibility joint with the 20th International Wroclaw Symposium on Electromagnetic Compatibility (EMC EUROPE). 2010. pp. 26–29.

Хоанг Лэ Чунг – магистрант, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, michael2102@mail.ru

Киричек Руслан Валентинович – кандидат технических наук, доцент, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, kirichek@sut.ru

Hoang Le Trung – Postgraduate, SPbSUT, St. Petersburg, 193232, Russian Federation, hoangtrung@spbgut.ru

Kirichek Ruslan – Candidate of Engineering Sciences, docent, SPbSUT, St. Petersburg, 193232, Russian Federation, kirichek@sut.ru