УДК 629.735.05

ОЦЕНКА УРОВНЯ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Игорь Мачалин, Петр Андрухович, Александр Пузыренко, Ирина Терентьева

В процессе построения комплексных систем защиты информации корпоративных сетей необходимо проводить анализ и оценку возможных утечек информации за счет побочных электромагнитных излучений от различных источников. В настоящее время, модели оценки угроз утечки информации за счет побочных излучений имеют обобщенный характер и отсутствуют адекватные аналитические модели, позволяющие оценить уровень побочных излучений в заданных точках внутри помещения и снаружи. Отсутствуют аналитические аппроксимации напряженности электромагнитных полей. При этом получить числовые оценки защищенности можно только путем экспериментальных исследований. На основе практического эксперимента были проведены измерения уровней побочного излучения на различных расстояниях от источника излучения и в широком диапазоне частот. Для исследуемой корпоративной сети выполнена сплайн-аппроксимация экспериментальных данных, на основе которой получены аналитические выражения для оценки затухания поля на исследуемых частотах путем усовершенствования модели Хата. Проведенное сопоставление экспериментальных данных и аналитических расчетов показало адекватность математической модели. Разработанные модели позволяют аналитически оценивать уровень побочных излучений корпоративных сетей и могут использоваться в процессе разработки и построения комплексных систем защиты информации.

Ключевые слова: *утечка информации, затухание сигналов, побочные излучения, коэффициент затуханий, модель Хата.*

Постановка проблемы. В настоящее время проблема обеспечения безопасности информационных технологий занимает все более значительное место в использовании информационно-коммуникационных систем и сетей по мере того, как растет их роль в информатизации общества. Особую актуальность эта проблема имеет при защите информационных ресурсов корпоративных сетей. Для построения комплексных систем защиты информации необходимо знать, как распространяется электромагнитное поле от того или иного источника и на какое расстояние. Только такой подход, учитывающий уровни побочных электромагнитных излучений (ПЭМИ) в сети позволит построить эффективную систему защиты. Таким образом, теория построения комплексных систем защиты информации с учетом влияния различных видов излучений является очень актуальным вопросом.

Анализ состояния проблемы и литературных источников. В настоящее время для оценки угроз безопасности и разработки политики безопасности организации используются внутренние методики, личный опыт, открытые публикации и рекомендации организаций, которые уже имеют опыт в этой области. В связи с этим возникают сомнения в корректности, полноте и качеству оценки угроз безопасности, а также в качестве разработки политики безопасности организации, поскольку не всегда учитываются физические каналы утечки информации за счет ПЭМИ. На данный момент, модели угроз информации за счет ПЭМИ имеют обобщенный характер и практически отсутствуют аналитические модели, позволяющие оценить уровень ПЭМИ в заданных точках внутри помещения и снаружи [1-4]. Отсутствуют аналитические аппроксимации напряженности электромагнитных полей. Поэтому получить числовые оценки защищенности можно только путем экспериментальных исследований. Таким образом, *целью статьи* является разработка математической модели оценки уровня утечки информации, за счет побочного электромагнитного излучения.

Постановка задач исследования. Как известно, в числе возможных каналов утечки информации, подлежащих защите, отдельное место занимает канал утечки за счет побочных электромагнитных излучений. Это определяется тем фактом, что практически каждое электротехническое устройство в процессе работы излучает в пространство электромагнитные волны, так или иначе связанные с его функционированием. Источниками излучения сигнала могут быть разные элементы изделий, которые осуществляют обработку информации. Основным источником побочных электромагнитных излучений может выступать компьютер и комплектующие, которые он использует.

Для персонального компьютера (ПК) высокочастотные излучения находятся в диапазоне до 1 ГГц с максимумом в полосе 50 ... 300 МГц. Широкий спектр обусловлен наличием как основной, так и высших гармоник последовательно-

стей коротких прямоугольных информационных импульсов. К появлению дополнительных составляющих в побочном электромагнитном излучении приводит также применение в вычислительных средствах и сетях высокочастотной коммутации.

Говорить о какой-либо диаграмме направленности электромагнитных излучений ПК не имеет смысла, потому что расположение его составных частей имеет много комбинаций. При этом поле, излучаемое ПК имеет линейную поляризацию. Она определяется расположением соединительных кабелей, являющихся основными источниками излучений в ПК с металлическим кожухом на системном блоке. Уровни побочных электромагнитных излучений регламентированы по условиям электромагнитной совместимости целым рядом зарубежных и отечественных стандартов. Так, например, согласно публикациям [4, 5], для диапазона 230...1000 МГц уровень напряженности электромагнитного поля, излучаемого оборудованием, на расстоянии 10 м не должен превышать 37 дБ. Однако излучения такого уровня могут быть перехвачены на значительных расстояниях. Следовательно, соответствие электромагнитных излучений средств нормам на электромагнитную совместимость не обеспечивает конфиденциальности обрабатываемой в них информации.

Не все составляющие спектра ПЭМИ персональных компьютеров являются опасными с точки зрения утечки информации. Спектр ПЭМИ современного электронного оборудования содержит гармоники в диапазоне частот до нескольких ГГц. Условно весь спектр излучений можно разбить на потенциально информативные и неинформативные излучения. Составляющие спектра ПЭМИ, порождаемые протеканием токов в цепях, по которым передаются содержащие конфиденциальную информацию сигналы, называют потенциально информативными ПЭМИ.

Для ПК потенциально информативными ПЭМИ являются излучения, которые сформированы следующими цепями: цепью передачи сигналов от контроллера клавиатуры к порту ввода-вывода на материнской плате; цепями передачи видеосигнала от видеоадаптера до электродов электронно-лучевой трубки монитора; цепями формирования данных системной шиной компьютера; цепями формирования шины данных микропроцессора.

В большинстве цифровых устройств существуют цепи, выполняющие вспомогательные функции, содержащие конфиденциальную информацию. Излучения в таких цепях являются безопасными с точки зрения утечки информации. Для таких излучений подходит термин « неинформативные ПЭМИ». Неинформативные излучения могут сыграть положительную роль, так как могут служить препятствием для приема информативных ПЭМИ при совпадении диапазона частот. К безопасным информативных излучений ПК можно отнести излучения цепей формирования шины данных системной шины и шину данных микропроцессора, а также излучение других цепей передачи информации в многоразрядном параллельном коде. Таким образом, основным направлением исследования являются уровни информативного и неинформативного ПЭМИ и оценка затуханий излучений.

Методика оценки затуханий. Для исследования уровней затухания и напряженности поля был проведен практический эксперимент. В качестве источника излучения исследовался компьютер типа IBM PC / AT (в частности монитор). Он располагался на втором этаже здания. Здание типовой конструкции имеет в своем составе два корпуса, соединенных переходом. Исследуемый объект располагался в первом корпусе. Корпус трехэтажный, блочно-панельный, высота каждого этажа с учетом межэтажных перекрытий – 4 м. В помещениях здания расположены письменные столы, а также контрольно-измерительная аппаратура. В качестве информации, которая обрабатывалась на компьютере, использовалась тестовая программа, в ходе работы которой были задействованы в циклическом режиме системный блок и монитор. Компьютер располагался на рабочем столе, на расстоянии 1 м от окна. Были проведены измерения напряженности электромагнитного поля на различных расстояниях от источника излучения и на разных частотах: 30 МГц (частота К1); 50 МГц (частота К2); 100 МГц (частота К3); 130 МГц (частота К4); 150 МГц (частота К5); 185 МГц (частота К6); 230 МГц (частота К7); 300 МГц (частота К8); 500 МГц (частота К9); 700 МГц (частота К10); 900 МГц (частота К11); 1000 МГц (частота К12).

Напряженность электромагнитного поля, создаваемого исследуемым источником, фиксировалась с помощью набора откалиброванных антенн, подключенных к входу измерительного приемника. В качестве измерительного приемника использовался селективный микровольтметр

типа SMV – 8.5. Коэффициент затухания рассчитывался по формуле: $K_{дБ} = 20\lg\left(\frac{E_d}{E_0}\right)$, где K – коэффициент затухания электрического поля, создаваемого исследуемым источником излучения; E_0 – напряженность поля, измеренная на расстоянии 0,5 м от источника; E_d – напряженность поля, измеренная на расстоянии d от источника излучения.

По результатам исследования были построены графические зависимости коэффициента затухания ПЭМИ от расстояния для всех исследуемых частот. На рис. 1 и рис. 2 приведены зависимости коэффициента затухания ПЭМИ от расстоянии d для частот К1 и К2.

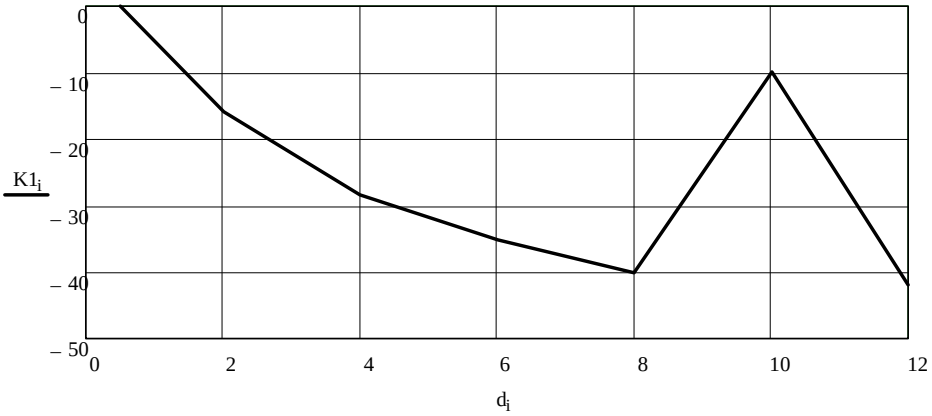

Рис. 1. Зависимость коэффициента затухания ПЭМИ от расстояния на частоте К1

На основе приведенных измерений можно сделать вывод, что закон затухания поля в пространстве зависит от ряда внешних факторов. Так, с увеличением расстояния (рис. 1) наблюдается рост коэффициента затухания, чего теоретически не должно происходить. Это обусловлено наличием в пространстве, окружающем источник излучения, инородных тел, а также проявлением таких явлений, как экранирование, переизлучение и т.д.

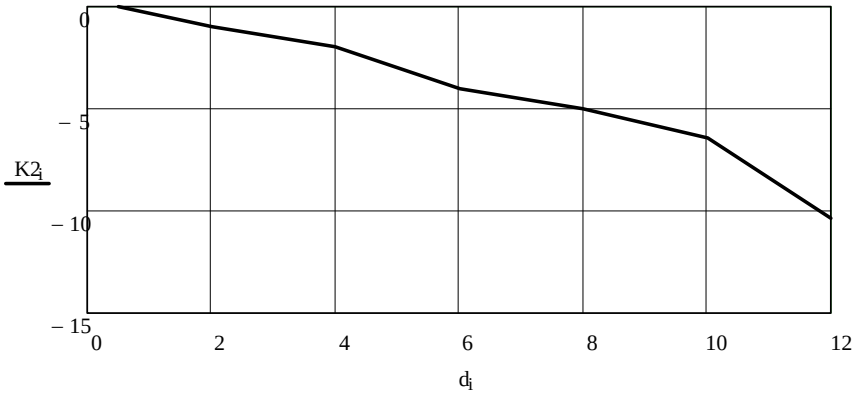

Рис.2. Зависимость коэффициента затухания ПЭМИ от расстояния на частоте К2

Все это приводит к неожиданным всплескам электрического поля, которые наблюдаются на графике. На частоте К2 (рис. 2) эти явления менее выражены.

Поскольку на остальных исследуемых частотах (К3-К12) зависимости затухания от расстояния носят аналогичный (рис. 2) характер, далее они не приводятся

Поскольку затухание поля зависит от частоты излучения, было проведено исследование зависимости коэффициента затухания ПЭМИ от частоты. Дальнейшие расчеты были проведены по измерениям сделанными в точке Т2 (8 метров от источника).

Полученные значения коэффициента затухания электромагнитного поля при различных частотах приведены в табл. 1.

Далее была произведена обработка измеренных результатов и их аппроксимация с помощью сплайн-функций, что позволяет определить значения затуханий в промежуточных точках значений исследуемого частотного диапазона. Для получения искомой аналитической функции использовался полином третьей степени, который,

как показал анализ, обеспечивает достаточную точность аппроксимации. Полином имеет вид:

$$y = a1x^3 + a2x^2 + a3x + a4.$$

Таблица 1

Значения коэффициента затухания электромагнитного поля в точке Т2

Частота излучения источника, МГц	Значение коэффициента затухания электромагнитного поля в точке Т2, дБ
30	-40
50	-5
100	-46
130	-78
150	-82
185	-52
230	-30
300	-11.2
500	-25
700	-24
900	-37
1000	-44

Для уменьшения объема вычислений диапазон частот 30-1000 МГц разделен на три поддиапазона: от 30 до 130 МГц; от 130,1 до 300 МГц: от 300,1 до 1000 МГц.

На основании данных, полученных в результате измерений, с использованием встроенных функций прикладного пакета MATHCAD получены коэффициенты $a1, a2, a3, a4$ для различных поддиапазонов. Так для первого поддиапазона значения коэффициентов:

$$V = \begin{matrix} 2,256\cdot 10^{-4} \\ -0,063 \\ 4,865 \\ -117,554 \end{matrix}.$$

На основании модели Хата [2] получена аналитическая зависимость затуханий для первого диапазона частот:

$$L_f = 2,256\cdot 10^{-4} f^3 - 0,063 f^2 + 4,865 f - 117,554.$$

Аналогичным образом получены аналитические выражения для остальных поддиапазонов частот. Таким образом, можно записать:

$$L_f = \begin{cases} 2,256\cdot 10^{-4} f^3 - 0,063 f^2 + 4,865 f - 117,554 & 30МГц \le f < 130МГц \\ 2,467\cdot 10^{-5} f^3 - 0,019 f^2 + 4,988 f - 461,464 & 130МГц \le f < 300МГц \\ -1,417\cdot 10^{-7} f^3 + 1,85\cdot 10^{-4} f^2 - 0,078 f - 4,75 & 300МГц \le f \le 1000МГц \end{cases}.$$

В табл. 2 приведены значения измеренных затуханий и значения затуханий, рассчитанные по аналитической формуле, как видно аналитические результаты достаточно хорошо сходятся с практическими измерениями, относительная ошибка не превышает 5%. Что подтверждает адекватность предложенной аналитической модели.

Таблица 2

Сравнительные значения затуханий

Частота излучения, МГц	Значение измеренных затуханий, дБ	Значения затуханий, рассчитанные по аналитической формуле, дБ
30	22	22,213
50	3	3,6
100	33	35,454
130	50	54,161
150	57	57,503
185	32	32,758
230	18	19,161
300	7	8,974
500	15	15,212
700	17	17,303
900	28	28,399
1000	39	39,45

Выводы. В статье представлены исследования канала утечки информации за счет ПЭМИ. На основе практического эксперимента были проведены измерения напряженности электрического поля на различных расстояниях от источника излучения и на разных частотах в диапазоне от 30 МГц до 1000 МГц. На основе проведенных измерений был построен ряд зависимостей коэффициента затухания поля от расстояния и частоты. Сплайн-аппроксимация данных зависимостей позволяет провести усовершенствование модели Хата для моделирования каналов утечки информации в рабочих помещениях. Получены математические модели для оценки затуханий на произвольных частотах. Проведенное сопоставление экспериментальных данных и аналитических расчетов показало адекватность математической модели. Результаты могут использоваться в процессе проектирования и эксплуатации комплексных средств защиты информации. Дальнейшим развитием этих результатов является исследование других моделей затуханий излучений с целью получения более универсальных математических выражений.

ЛИТЕРАТУРА

[1]. Галатенко В.А. Информационная безопасность/ В.А. Галатенко // Открытые системы.-№4. – 1995. – С. 17-23.

[2]. Конахович Г.Ф. Захист інформації в телекомунікаційних системах/Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов//–К.:НАУ, 2007. – 321 с.

[3]. Генне В.И. Защита информации от утечки через побочные электромагнитные излучения цифрового электронного оборудования/ В.И. Генне //Конфидент. –№2. –1988. – С. 8-12.

[4]. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебное пособие/Г.А. Бузов, С.В. Калинин, А.В. Кондратьев / М.: Горячая линия-Телеком, 2005. – 416 с.

[5]. Руководящий документ. Руководство по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России / Информационная безопасность. –№1. – 2006. – С.1-6.

REFERENCES

[1]. Galatenko V.A. (1995) Information Security., Open Systems, No.4, pp. 17-23.

[2]. Konakhovich G.F., Klimchuk G.F., Pauk S.M., Potapov V.G., (2007), Data protection in telecommunication systems, Kyiv, NAU, 321 p.

[3]. Henne V.I.(1988), Data Protecting from losses via electromagnetic radiation side of digital electronic equipment, Confident, No.2, pp. 8-12.

[4]. Buzov G.A., Kalinin S.V., Kondratyev A.V., (2005), Protection against leakage of information through technical channels, Moscou, Hotline-Telecom, 416 p.

[5]. Guidance document. Guidelines for the development of protection profiles and security assignments. Russian State Technical Commission (2006), Information Security, No.1, pp.1-6.

ОЦІНКА РІВНЯ ВИТОКУ ІНФОРМАЦІЇ ЗА РАХУНОК ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ

У процесі побудови комплексних систем захисту інформації корпоративних мереж необхідно проводити аналіз і оцінку можливих витоків інформації за рахунок побічних електромагнітних випромінювань від різних джерел. В даний час, моделі оцінки загроз витоку інформації за рахунок побічних випромінювань мають узагальнений характер і відсутні адекватні аналітичні моделі, що дозволяють оцінити рівень побічних випромінювань в заданих точках всередині приміщення і зовні. Відсутні аналітичні апроксимації напруженості електромагнітних полів. При цьому отримати числові оцінки захищеності можна тільки шляхом експериментальних досліджень. На основі практичного експерименту були проведені вимірювання рівнів побічного випромінювання на різних відстанях від джерела випромінювання і в широкому діапазоні частот. Для досліджуваної корпоративної мережі виконана сплайн-апроксимація експериментальних даних, на основі якої отримано аналітичні вирази для оцінки загасання поля на досліджуваних частотах шляхом удосконалення моделі Хата. Проведене зіставлення експериментальних даних і аналітичних розрахунків показало адекватність математичної моделі. Розроблені моделі дозволяють аналітично оцінювати рівень побічних випромінювань корпоративних мереж і можуть використовуватися у процесі розробки та побудови комплексних систем захисту інформації.

Ключові слова: витік інформації, загасання сигналів, побічні випромінювання, коефіцієнт затуханий, модель Хата.

ASSESSMENT OF INFORMATION LOSSES LEVEL DUE TO ADVERSE ELECTROMAGNETIC RADIATION

In the process of building complex systems of information protection of corporate networks is necessary to analyze and evaluate possible losses due to stray electromagnetic radiation from various sources. Currently, the models of threat assessment information leakage due to spurious emissions are generic in nature and there are no adequate analytical models to assess the level of spurious emissions at given points inside and outside. No analytical approximation of electro-magnetic fields. In this case, get the numerical evaluation of security is only possible by experimental studies. Based on practical experiments were conducted measuring the levels of spurious emissions at different distances from the radiation source in a wide frequency range. To study the corporate network is made of spline approximation of the experimental data on which to base the analytical expressions for estimating the field attenuation at frequencies investigated by improving the Hata model. The comparison of experimental data and analytical calculations showed the adequacy of the mathematical model. The developed models can analytically evaluate the level of spurious corporate networks and can be used in the design and construction of complex security systems.

Keywords: information losses, signal attenuation, spurious emissions, attenuation coefficient, the model Hut

Мачалін Ігор Олексійович, доктор технічних наук, доцент, професор кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: igor.machalin@ukr.net

Мачалин Игорь Алексеевич, доктор технических наук, доцент, профессор кафедры телекоммуникационных систем Национального авиационного университета.

Machalin Igor, Doctor of Science in Eng., Professor of Academic Department of Telecommunication systems, National Aviation University.

Пузиренко Олександр Юрійович, кандидат технічних наук, доцент кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: ajiekc1980@gmail.com
Пузыренко Александр Юрьевич, кандидат технических наук, доцент кафедры телекоммуникационных систем Национального авиационного университета.
Puzyrenko Alexander, PhD in Eng., associate professor of Academic Department of Telecommunication systems, National Aviation University.

Андрухович Петро Олександрович, старший викладач кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: peter.andrukhovich@gmail.com

Андрухович Петр Александрович, старший преподаватель кафедры телекоммуникационных систем Национального авиационного университета.
Andrukhovich Petr, Senior Lecturer of Academic Department of Telecommunication systems, National Aviation University.

Терентьєва Ірина Євгенівна, аспірант кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: i.terentyeva@ukr.net
Терентьева Ирина Евгеньевна, аспирант кафедры телекоммуникационных систем Национального авиационного университета.
Terentyeva Irina, postgraduated student of Academic Department of Telecommunication systems, National Aviation University.

УДК 681.3. 06 (07)

СУТНІСТЬ ЗАКОНОДАВЧИХ ОСНОВ ТА УМОВИ НАДАННЯ ДОВІРЧИХПОСЛУГ В ЕВРОПЕЙСЬКОМУ СОЮЗІ В ПЕРІОД 2015 – 2030 рр.

Юрій Горбенко

Розглядаються питання стану та необхідності удосконалення нормативно – правової законодавчої бази Європейського союзу (ЄС) відносно електронних довірчих операцій на внутрішньому ринку. Аналізуються основні положення "Регламенту Європейського Парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку". Робиться висновок про актуальність та необхідність приєднання України до електронного цифрового ринку ЄС та проведення відповідних досліджень та виконання розробок. Аналізується стан впровадження інфраструктури відкритого ключа, а в Україні системи ЕЦП, на практиці. Наводяться основні проблемні питаннями, що виникли в процесі застосування ЕЦП, - уніфікації, стандартизації, сумісності, масштабуємості, криптографічної стійкості, складності криптографічних перетворень тощо. Розробляються пропозиції, а також визначається сутність та визначаються умови відносно прийняття основних положень Регламенту для практичної реалізації, в тому числі на перспективу в Україні. Визначаються вимоги, які повинні бути вирішені в ЄС для надання безпечних електронних послуг щодо електронної ідентифікації, електронної автентифікації, електронного підпису, електронних печаток, електронних міток часу, електронних документів, послуг електронної доставки та перевірки справжності веб – сайту.

Ключові слова: *електронний цифровий ринок ЄС, електронні операції, механізми ідентифікації, автентифікації та електронні довірчі послуги.*

ВСТУП

Початок XXI століття характеризується інтенсивним впровадження інфраструктур відкритого ключа (ІВК) на практиці, основними завданнями яких стало виготовлення та обслуговування сертифікатів відкритих ключів для асиметричних криптографічних перетворень типу (електронний) цифровий підпис та направлений шифр [1, 2, 9]. Такі інфраструктури в основному є третіми довіреними сторонами. В Україні ІВК отримала назву системи електронного цифрового підпису (ЕЦП) [4]. Зрозуміло, що створення та застосування ІВК безпосередньо пов'язані з їх законодавчим та нормативно-правовим забезпеченнями. Історично спочатку в США [10], а потім і в ЄС [3] приймається закон (директива) та необхідний перелік нормативно-правових документів, що стосуються застосування (електронного) цифрового підпису та направленого шифрування. До того, як у 2000 р. президент США підписав закон «Про електронний цифровий підпис», практично в усіх штатах США він уже діяв, наприклад закон штату Юта «Про електронний цифровий підпис» був прийнятий в 1996 р. В