УДК 621.391

МЕХАНИЗМЫ И ПОСЛЕДСТВИЯ ПРЕДНАМЕРЕННЫХ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЙ НА ПЕРЕДАЧУ ДАННЫХ

Л.В. Баталов, М.И. Жуковский, Р.В. Киричек, Б.Н. Лазарев

Описаны механизмы и последствия преднамеренного электромагнитного воздействия на сети Ethernet с использованием сверхкоротких электромагнитных импульсов. Представлена вероятностная модель возникновения ошибок при передаче данных в сети Ethernet при таких воздействиях.

Ключевые слова: защита информации, электромагнитные воздействия, сверхкороткие импульсы, вероятности ошибок.

Введение

Преднамеренные электромагнитные воздействия (ПД ЭМВ) являются новым фактором угроз информационной безопасности ключевых объектов информационной инфраструктуры. Эту угрозу следует оценивать как долговременную, требующую принятия адекватных защитных мер со стороны государства и общества.

ПД ЭМВ наиболее эффективны при реализации их двумя способами:

- электромагнитным полем;
- по проводным линиям связи.

При этом наибольшую опасность представляют воздействия, имеющие относительно невысокую энергию и близкие по своим параметрам к полезному сигналу, передаваемому по линиям связи в сети Ethernet. Эти воздействия могут быть реализованы с использованием генераторов сверхкоротких электромагнитных импульсов (СК ЭМИ), технология создания которых стремительно развивается в последние годы.

К настоящему времени получено большое количество экспериментальных и теоретических результатов, подтверждающих высокую эффективность применения СК ЭМИ для искажения, уничтожения

и блокирования информации. Работы в направлении создания систем защиты, систем обнаружения электромагнитных атак требуют глубокого знания и понимания тонких механизмов работы IT-систем.

В работе приведены некоторые результаты разработки вероятностной модели возникновения ошибок при передаче данных в сетях Ethernet в условиях воздействия СК ЭМИ на физическую среду.

Механизм ПД ЭМВ на передачу данных

Сегодня повсеместно используемой технологией построения локальных сетей является Ethernet. В подавляющем большинстве для данной технологии на физическом уровне в качестве физической среды передачи данных, в основном, используется неэкранированная медная витая пара категории 5e [1]. В результате ПД ЭМВ электромагнитным полем или по проводным линиям связи с помощью генераторов-инжекторов уровень наведенных помех становится сопоставимым с уровнем информационных сигналов, что может приводить к разрушению обрабатываемой информации. На рис. 1 показан механизм возникновения ошибок при передаче сигналов в двоичном (манчестерском) коде.

Рис. 1. Искажение битовой последовательности в результате ПД ЭМВ

В настоящее время наиболее распространенные стандарты – Fast Ethernet (трехуровневое кодирование), Gigabit Ethernet (пятиуровневое кодирование) для спецификаций 100Base-TX и 1000Base-T соответственно – не используют алгоритмы кодирования с коррекцией ошибок, поэтому искажение даже одного символа в кадре ведет к ошибке приема всего кадра. Этот недостаток устранен в стандарте 10 Gigabit Ethernet (шестнадцатиуровневое кодирование), спецификация 10GBase-T, посредством применения избыточного кодирования с разреженной матрицей.

Вероятностные характеристики полезного сигнала в сети Ethernet

Для расчетных оценок вероятности возникновения ошибок при передаче сигналов в сетях Ethernet необходимы исходные данные по вероятностным характеристикам сигналов в физической среде передачи. Расчет этих характеристик проведем на основе упрощенной математической модели кодированной последовательности, базирующейся на следующих основных положениях:

- исходная (не кодированная) последовательность битов $x = (x_1 \ldots x_n)$, $x_i = (0,1)$, $i = 1,2 \ldots n$ является случайной, состоящей из независимых одинаково распределенных величин. Полагаем, что вероятности появления нуля и единицы равны ½;
- кодированная последовательность $y = (y_1 \ldots y_n)$ является стационарной в широком смысле и эргодичной;
- схема кодирования $x \rightarrow y$ не вносит в выходную последовательность y ошибок;
- значения помехи много больше уровня фонового шума в информационном канале. По этой причине аддитивный фоновый шум в данной работе не учитывается.

Алгоритм кодирования удобно представить в виде графа-дерева, в корне которого стоит символ y_1, а n-й ярус представляет собой множество символов $\{y_n\}$, в которые может привести этот алгоритм через n шагов. Каждой ветви графа приписывается вес – соответствующая вероятность перехода. Всего таких графов имеется q – по алфавиту кодирования «леса», поэтому все характеристики необходимо также усреднять по возможным y_1. Тогда нахождение всех вероятностных характеристик сводится к нахождению величин $z_1(n)$, …, $z_q(n)$ – числа символов, соответствующего i-ой букве алфавита $z_i(n)$. Как правило, для этих величин можно написать рекуррентное соотношение [2], связывающее их с подобными величинами на предыдущих уровнях.

Можно показать, что, например, для алгоритма MLT-3, применяемого для передачи данных по витой паре в стандарте Fast Ethernet [2],

$$\lim_{n\to\infty} P^n = \begin{pmatrix} 1/4 & 1/2 & 1/4 \\ 1/4 & 1/2 & 1/4 \\ 1/4 & 1/2 & 1/4 \end{pmatrix},$$

где P^n – матрица переходных вероятностей, поэтому вероятности появления символов (–1,0,1) равны соответственно (1/4,1/2,1/4). Усредняя по начальным состояниям, находим для MLT-3 коэффициент корреляции между 1-ым и (1+n)-ым символом

$$K_n = P^n(1,1) - P^n(3,1) = 2^{-\frac{n+1}{2}} \sin\frac{\pi}{4}(n+1). \qquad (1)$$

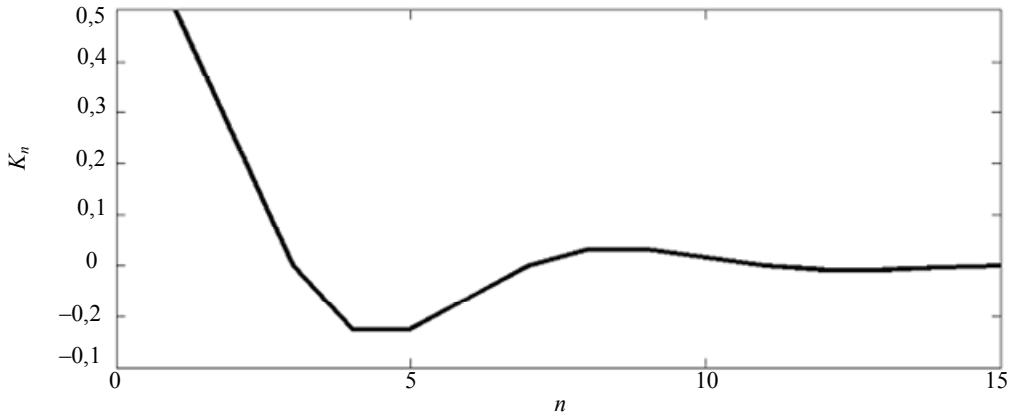

Рис. 2. Коэффициент корреляции между символами

На рис. 2 приведен коэффициент корреляции K_n для n = 1–15. Видно, что алгоритм кодирования имеет «память», так как имеется корреляция между символами, отстающими друг от друга на некоторое расстояние. Множитель $2^{-(n+1)/2}$ в (1) отвечает общему убыванию функции K_n, а второй множитель $\sin(\pi\times(n+1)/4)$ обеспечивает осцилляции. Это приводит к появлению бесконечного числа локальных экстремумов зависимости K_n. Наиболее велик первый локальный минимум, равный –1/8. Приведем первые семь значений:

K_n = 1/2, 1/4, 0, –1/8, –1/8, –1/16, 0… (2)

Авторами проведен статистический анализ реальных осциллограмм электрических сигналов Fast Ethernet различных типов трафика, передаваемого по сети. В результате анализа на цифровом осциллографе были записаны образы сигналов в линии связи. Полученные осциллограммы были обработаны с помощью пакета MATLAB 2009b (рис. 3).

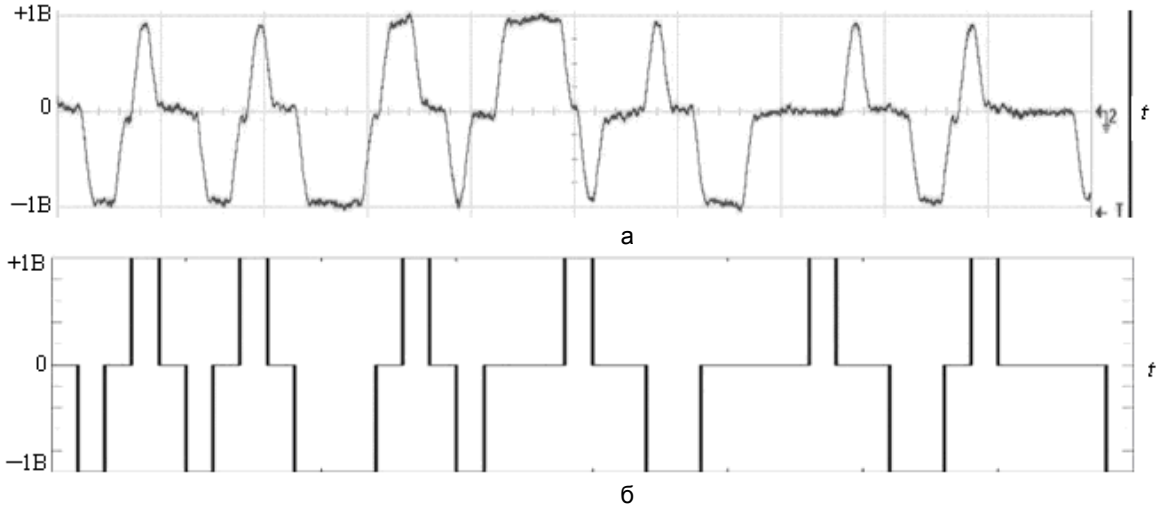

Рис. 3. Результат обработки фрагмента осцилограммы в пакете MATLAB для спецификации 100Base-TX: осциллограмма сигнала в линии связи (а); представление сигнала после обработки в пакете MATLAB (б)

Тип трафика	K_1	K_2	K_3	K_4	K_5
Потоковый	0,49	0,23	0,009	–0,12	–0,11
Сигнальный	0,49	0,23	0,012	–0,12	–0,12
Интерактивный	0,49	0,23	0,008	–0,12	–0,12
Передачи данных	0,50	0,23	0,013	–0,12	–0,11

Таблица 1. Экспериментальные значения коэффициентов корреляции

Восстановление из электрического сигнала последовательности символов (–1, 0, 1) проводилось с помощью специального алгоритма прореживания, который включает в себя фильтр нижних частот. Вероятности появления символов, найденные теоретически (0,25; 0,5; 0,25), близки к найденным экспериментально. Эти значения вероятностей можно рекомендовать для анализа влияния преднамеренных деструктивных электромагнитных воздействий на передачу данных в сетях Ethernet, использующих кодирование MLT-3 [3]. В табл. 1 приведены значения коэффициентов корреляции K_n, также полученные экс-

периментально для различных типов трафика, которые, как нетрудно убедиться, близки к вышеприведенным теоретическим значениям (2). Важным результатом является подтвержденная экспериментально практическая независимость статистических характеристик, в том числе вероятностей появления символов, от типа идущего по сети трафика.

Вероятности ошибок передачи при ПД ЭМВ

Из анализа возможных ошибок, возникающих в сетях Ethernet при воздействии СК ЭМИ [3], следует, что наиболее вероятным типом ошибок является передача кадра с повреждением (ошибка в контрольной сумме FCS). Предлагается оценивать снижение производительности сетей Ethernet путем оценки интенсивности возникновения данного типа ошибок.

Для этого рассмотрена простейшая сеть Ethernet, которая может быть представлена в виде двух компьютеров (передающего и принимающего информацию) и линии передачи данных (кабеля). Передаваемые данные представляют собой периодическую последовательность кодовых посылок различных уровней напряжения, образующуюся путем ряда преобразований исходного сигнала. Если напряжение импульсной помехи накладывается на электрические символы, то их значение может быть воспринято некорректно. Этот эффект называется единичным сбоем, и его вероятность обозначается P_e.

Предположим, что помеха $V(t)$ представляет собой последовательность импульсов, следующих друг за другом с частотой f (рис. 4).

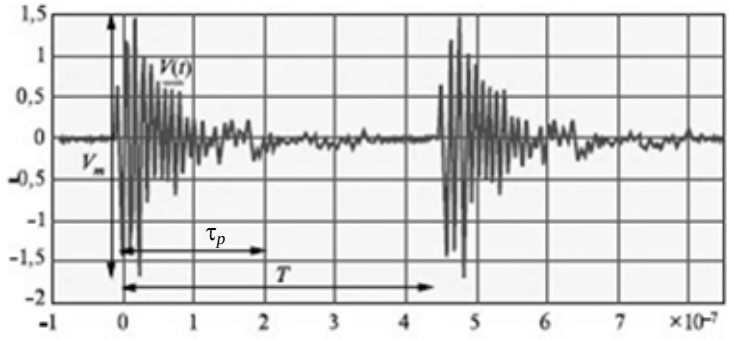

Рис. 4. Типовая осциллограмма СК ЭМИ, наведенных в линии связи

Тогда $V(t)$ можно преобразовать в эквивалентное напряжение гауссовского шума V_{ng} при условии равенства энергий этих помех [4]:

$$V_{ng}{}^2 = \frac{1}{\mathrm{T}}\int_0^T V^2(t)\,dt = V_{\mathrm{м}}{}^2 \cdot f \cdot K,$$

где $V_{\mathrm{м}}$ – амплитуда импульса; $K = \int_0^{\tau_{\mathrm{p}}} g^2(t)\,dt$; $g(t)$ – форма импульса; τ_{p} – длительность импульса.

Пусть кадр передаваемых данных состоит из N битов, а символьная скорость равна R. Тогда $m=(f\cdot N/R)(\tau_{\mathrm{p}}\cdot R)=f\tau_{\mathrm{p}}N$ битов будут подвержены воздействию. Вероятность того, что подверженный воздействию бит информации будет воспринят правильно, равна $Q = 1–P_e$, а вероятность неправильной передачи кадра данных в результате единичного сбоя равна

$$P_{\mathrm{loss}} = 1-\left(1-P_{\mathrm{e}}(z)\right)^m = 1-\left(1-P_{\mathrm{e}}(z)\right)^{f\tau_{\mathrm{p}}N}.$$

Были рассмотрены различные схемы кодирования, применяемые в указанных выше наиболее распространенных спецификациях Ethernet (Fast Ethernet, Gigabit Ethernet и 10 Gigabit Ethernet). Ниже приведены полученные формулы для расчета вероятности того, что принимаемый кадр будет потерян для спецификации 100Base-TX (3), 1000Base-T (3) и 10GBase-T (5).

$$P_{loss} = 1-\left(0,5-0,25\,\mathrm{erf}\left(\frac{1,202}{V_{\mathrm{M}}\sqrt{f\tau_{\mathrm{p}}}}\right)+0,75\,\mathrm{erf}\left(\frac{1,2121}{V_{\mathrm{M}}\sqrt{f\tau_{\mathrm{p}}}}\right)\right)^m, \quad (3)$$

$$P_{loss} = 1-\left(\frac{1+\mathrm{erf}\left(\frac{1,75}{V_{\mathrm{M}}\sqrt{f\tau_{\mathrm{p}}}}\right)+\mathrm{erf}\left(\frac{1,25}{V_{\mathrm{M}}\sqrt{f\tau_{\mathrm{p}}}}\right)+\mathrm{erf}\left(\frac{0,75}{V_{\mathrm{M}}\sqrt{f\tau_{\mathrm{p}}}}\right)+\mathrm{erf}\left(\frac{0,25}{V_{\mathrm{M}}\sqrt{f\tau_{\mathrm{p}}}}\right)}{5}\right)^m, \quad (4)$$

$$P_{loss} = 1 - \sum_{k=0}^{h(SNR)} C_m^k P_e^k \left(1 - P_e\right)^{m-k}, \quad (5)$$

где m – число символов, подверженных воздействию; $h(SNR)$ – максимальное число искаженных символов, при котором кадр будет востановлен и принят корректно.

На основе рассмотренной взаимосвязи качества обслуживания [5] и устойчивости сетей Ethernet [6] удалось сформировать перечень критичных параметров – вероятности потерь кадров P_{loss}, скважности S и амплитуды помехи A – для рассмотренных спецификаций Ethernet.

На основании полученных вероятностей была решена обратная задача и получены параметры устойчивости рассматриваемых спецификаций Ethernet (рис. 5).

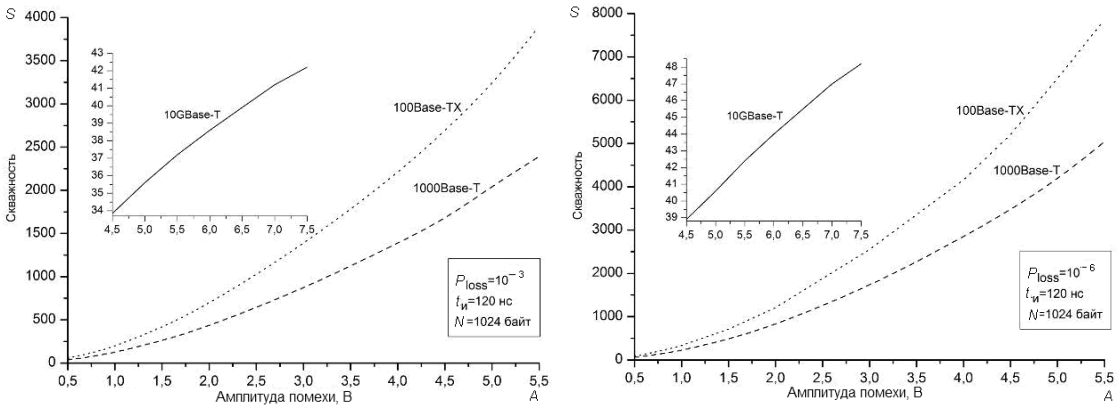

Рис. 5. Устойчивость сетей Ethernet в зависимости от амплитуды и скважности: вероятность потерь кадров 10^{-3} (а); вероятность потерь кадров 10^{-6} (б)

Для проверки адекватности расчетного аппарата был проведен натурный эксперимент. В проводной линии связи наводилась помеха с параметрами: амплитуда импульсов 5 В, их длительность 200 нс, частота повторения 5 кГц. Сопоставление экспериментально полученной в натурных экспериментах доли потерянных кадров с результатами расчетов последствий воздействия помехи с аналогичными параметрами приведено в табл. 2.

Технология	Длина кадра					
	64 байт		768 байт		1518 байт	
	теор.	эксперим.	теор.	эксперим.	теор.	эксперим.
Fast Ethernet 100Base-TX	0,17	0,16	0,33	0,31	0,50	0,54
Gigabit Ethernet 1000Base-T	0,21	0,19	0,36	0,35	0,54	0,58
10 Gigabit Ethernet 10GBase-T*	0	0	0,12	0,09	0,26	0,21

*Данные получены путем имитационного моделирования в MATLAB Simulink

Таблица 2. Доля потерянных кадров

Видно хорошее соответствие полученных результатов и теоретических расчетов.

Заключение

Преднамеренные электромагнитные воздействия могут приводить к ошибкам при передаче данных в сетях Ethernet. Анализ механизмов возникновения ошибок позволил предложить вероятностную математическую модель их возникновения при воздействии сверхкоротких электромагнитных импульсов, основываясь на представлении воздействия в виде эквивалентного гауссова шума. С учетом особенности кодировки в спецификациях 100Base-TX, 1000Base-T, 10GBase-T предложены соотношения, позволяющие рассчитать вероятности неправильной передачи пакета данных при известных параметрах наведенных периодических импульсных помех. Это позволит анализировать эффективности воздействия сверхкоротких электромагнитных импульсов на процесс передачи данных в сети Ethernet и формулировать рациональные требования к оборудованию для защиты данных от электромагнитных воздействий.

Литература

1. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство. – 3-изд. – М.: Вильямс, 2008. – 1168 с.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Питер, 2011. – 944 с.

3. Киричек Р.В., Лазарев Б.Н., Баталов Л.А. Вероятностные характеристики сигналов Ethernet // Сборник трудов Межвузовской научно-практической конференции с международным участием «Актуальные проблемы организации и технологии защиты информации». – СПб: СПбГУ ИТМО, 2011. – С. 135–139.
4. Вегешна Шринивас. Качество обслуживания в сетях IP: Пер. с англ. – М.: Вильямс, 2003. – 368 с.
5. Kohlberg I. and R.J. Carter. Some theoretical considerations regarding the susceptibility of information systems to unwanted electromagnetic signals // Proc. of the 14th Int. Zurich Symposium on EMC. – Zurich, Switzerland, 2001. – February 20–22. – P. 41–46.
6. Приказ Минкомсвязи РФ от 27.09.2007. № 113. «Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования».

Баталов Лев Алексеевич – ФГУП «ЦентрИнформ», инженер-программист, l.batalov@center-inform.ru
Жуковский Михаил Иванович – ФГУП «ЦентрИнформ», кандидат технических наук, начальник НИИЦ, m.zhukovsky@center-inform.ru
Киричек Руслан Валентинович – ФГУП «ЦентрИнформ», старший научный сотрудник, r.kirichek@center-inform.ru
Лазарев Борис Николаевич – ФГУП «ЦентрИнформ», кандидат технических наук, старший научный сотрудник, начальник группы, tiger50@mail.ru