Список використаної літератури: ***1****. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.: Кн.1. М.: Энергоатомиздат, 1994. 400 с.* ***2****. Антонов А. В. Системный анализ. Методология. Построение моделей: Учебное пособие. Обнинск: ИАТЭ. 2001. 272 с.* ***3.*** *Домарев В. В. Безопасность информационных технологий: Методология создания систем защиты. К.: ООО "Тид "ДС". 2001. 688 с.* ***4.*** *Колмогоров А. Н., Драгалин А. Г. Введение в математическую логику. М.: Изд-во МГУ, 1982. 120 с.* ***5****. Хорев А. А. Способы и средства защиты информации: Учебное пособие. М.: МО РФ, 1998. 315 с.* ***6.*** *ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.* ***7.*** *Богуш В. М., Кудін А. М. Інформаційна безпека від А до Я. 3000 термінів і понять – К.: МОУ, 1999. – 456 с.* ***8.*** *Технические средства и методы защиты информации. Учебное пособие для вузов/ А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков и др.; под ред. А. П. Зайцева и А. А. Шелупанова. – 4-е изд., испр. и доп. – М.: Горячая линия-Телеком, 2012. – 616 с: ил.* ***9.*** *Богуш В. М., Юдін О. К. Інформаційна безпека держави. – К.: "МК-Прес", 2005. – 432 с., іл.* ***10.*** *Богуш В. М. Розвідка в інформаційному суспільстві: Довідник-словник. – К.: МОУ, 2000. – 768 с.*

Михаил Прокофьев, Василий Стеченко
НДЦ «ТЕЗИС» НТУУ КПИ

УДК 621.372

ОЦЕНКА ВЕРОЯТНОСТИ ПРАВИЛЬНОГО РАСПОЗНАВАНИЯ ИНФОРМАЦИИ ПРИ ПРИЕМЕ ПОБОЧНОГО ИЗЛУЧЕНИЯ ОТ ПАРАЛЛЕЛЬНО ПЕРЕДАВАЕМЫХ СИГНАЛОВ

Анотація: ***Показано шлях розрахунку ймовірності правильного прийому одиниці інформації залежно від відношення сигнал/шум для сигналів з паралельним кодуванням інформації.***
Summary: ***Shows the calculation of the probability of correct reception of units of information, depending on the signal / noise ratio for signals with parallel coding information***
Ключевые слова: ***Защита информации, параллельное кодирование информации.***

I Введение

В средствах вычислительной техники часто применяется параллельная передача информационных сигналов по многопроводному кабелю. Информация передается с помощью электрических сигналов, поэтому в окружающее пространство излучается электромагнитное поле, которое может быть перехвачено средствами технической разведки.

В многопроводном кабеле по n линиям синхронно передаются n двоичных сигналов с потенциальным кодированием информации. Обычно высоким уровнем сигнала кодируется «1», а низким - «0». Средства технической разведки принимают сигнал побочного излучения от всех проводов кабеля, что затрудняет задачу идентификации сигналов в каждом проводе кабеля. О большей защищенности информации при параллельной ее передачи указывается в работах [1, 2], однако численные сравнения отсутствуют. Оценке вероятности правильного приема бита информации при параллельной передаче сигналов и посвящена настоящая статья.

II Основная часть

Количественной характеристикой качества передачи информации является вероятность ее правильного приема, например, вероятность правильного приема одного бита информации. Такая оценка определяет среднее число правильно расшифрованных битов при распознавании принятого сигнала.

Информационные сигналы побочного излучения принимаются на некотором расстоянии без прямого подключения к проводам многопроводной линии. В результате на вход приемного устройства поступает суммарный сигнал, излученный всеми проводами многопроводной линии. По результатам измерения этого суммарного сигнала необходимо определить значение переданных символов в каждой линии.

За один такт количество передаваемых многопроводной линией информационных битов совпадает с количеством сигнальных проводов в линии n. В зависимости от номера линии и уровня передаваемого сигнала (высокий – «1», низкий – «0») общее количество возможных вариантов комбинаций символов, которое одновременно передается многопроводным кабелем, равно 2^n. При передаче электрического сигнала в пространство излучается электромагнитное поле и уровень излученного сигнала может изменяться в больших пределах. Минимальный уровень излучения будет при передаче по всем линиям «0», а

максимальный – при передаче «1». Для декодирования принятой комбинации сигналов необходимо не только правильно измерить уровень суммарного сигнала, но и распознать сигнальные провода, в которых передавались сигналы «1». Одновременно необходимо учитывать мешающее влияние шума, который вместе с сигналом поступает на вход приемного устройства. В простейшем случае это сумма полезного сигнала и аддитивной помехи в виде стационарного гауссового шума с нормальным законом распределения амплитуды (белый шум).

Согласно теории потенциальной помехоустойчивости [3] минимум вероятности ошибки воспроизведения сигнала на выходе приемника при равновероятных сигналах обеспечивается оптимальным приемником, алгоритм работы которого имеет вид

$$\int_0^T [X(t) - S_i(t)]^2 dt \underset{S_i}{<} \int_0^T [X(t) - S_j(t)]^2 dt, \;\; i, j = 1,...,V; i \neq j. \tag{1}$$

где $X(t)$ – принимаемая смесь суммарного сигнала с шумом; $S_i(t)$ и $S_j(t)$ i-тая и j-тая копии принимаемых комбинаций сигнала.

Согласно этому выражению оптимальный приемник должен иметь 2^n каналов, в которых вычисляется квадрат расстояния

$$\left\| X - S_i \right\|^2 = \int [X(t) - S_i(t)]^2 dt, i,..., N, \tag{2}$$

между принимаемой комбинацией суммарного сигнала X и каждой i-той его копией S_i. Решение о принятой комбинации суммарного сигнала принимается по минимальному значению квадрата расстояния.

В типичных системах параллельной передачи сигналов уровни излученных сигналов от линий многопроводного кабеля практически одинаковы

$$| S_i(t) - S_j(t)| << | S_i(t)| \approx | S_j(t)|, \; i=1, \ldots, n, j=1, \ldots, n; \; i \neq j. \tag{3}$$

С учетом этого сравнение принятых комбинаций суммарного сигнала согласно (1) можно разделить на два этапа: определить группы с одинаковым количеством переданных сигналов высокого уровня (сигналов «1»), а потом устанавливать номера линий с высоким уровнем сигнала. Такое разделение позволяет уменьшить число каналов, в которых вычисляется квадрат расстояния между принятым сигналом и его возможной копией.

Количество возможных групп суммарного сигнала с одинаковым количеством «1» равно n+1, причем в каждой группе число комбинаций сигнала разное. Только одну комбинацию сигналов имеют группы, в которых передаются все «0» или все «1». Группы, имеющие один сигнал высокого уровня («1») или один сигнал низкого уровня, имеют n вариантов возможных комбинаций сигналов. Количество вариантов сигналов с двумя «1» или с двумя «0» равна $n\ (n - 1) / 2!$, а с произвольным числом «1» определяется как сочетание C_n^m, где m – число сигналов «1» в n параллельных линиях [4].

Уровни побочного излучения соизмеримы с уровнем маскирующего шума, поэтому чаще всего суммарный сигнал можно разделить только на отдельные группы по числу переданных «1». Оценим вероятность правильного приема одного бита информации при выполнении соотношения (3), то есть для одинаковых сигналов, излученных разными линиями. При оценке уровня суммарного сигнала можно сразу разделить его на две большие группы: с большим числом «1» и большим числом «0». Дальнейшее разделение на группы по числу принятых сигналов «1» не имеет смысла, поскольку при большем числе «1» в принятой комбинации будет приниматься решение о передаче во всех линиях сигналов «1», а при большем числе «0» – сигналов «0» во всех линиях.

Флюктуации шума будут приводить к появлению ошибок при разделении суммарного сигнала на две большие группы. Вероятность правильного разделения сигналов на группы в пороговом устройстве зависит от отношения энергии суммарного сигнала к спектральной плотности мощности помех $E/2N_0$ [3]. Если априорная информация о фазе, частоте и времени прихода сигнала известны и задачей обнаружения есть только установление факта приема сигнала, то вероятность правильного разделения определяется

$$P(x) = 0{,}5[1 + \Phi(x)], \tag{4}$$

где $\Phi(x)$ – функция Крампа; $x = \sqrt{(E/2N_0)}$ – корень из отношения энергии принятого суммарного сигнала E к удвоенной спектральной плотности мощности шума N_0. Энергия одиночного импульса $E = P_{ср}\tau$ – это произведение его средней мощности $P_{ср}$ на длительность τ. Спектральная плотность мощности «белого» шума $N_0 = P_ш/\Delta f$ – это отношение мощности шума $P_ш$ к полосе частот Δf, в которой эта мощность измерялась. Поэтому параметр $x = \sqrt{(P_{ср}/P_ш)}$ характеризует отношение сигнал/шум в принятом сигнале, где под уровнем

сигнала понимается корень из средней мощности принятого импульсного сигнала, а под уровнем шума – среднеквадратичное значение шума в полосе $\Delta f_э = 2/\tau$.

Будем считать, что коэффициент связи отдельных линий многопроводного кабеля достаточно мал и энергия суммарного сигнала равна сумме энергий отдельных сигналов. В этом случае уровень порога решающего устройства, в котором происходит разделение принятых комбинаций на две большие группы – это среднее значение уровня принятых сигналов $x_{пор} = nx_1/2$, где $x_1 = \sqrt{(E_1/2N_0)}$, а E_1 – энергия сигнала, который излучается одной линией.

Для нечетных значений n минимальная разность между порогом и уровнем двух ближайших групп сигналов $x_{min} = 0{,}5x_1$. Для следующих двух групп с числом передаваемых «1» $n/2 - 1{,}5$ и $n/2+1{,}5$ значение параметра x равно $1{,}5x_1$ и так далее. Для четных значений n значения порога $x_{пор} = nx_1/2$ совпадает с уровнем сигнала средней группы, а минимальное значение разностного сигнала равно x_1. Максимальная разность между пороговым уровнем и уровнем принятого сигнала будет для комбинаций суммарного сигнала, когда по всем линиям передаются «0» или «1».

Вероятность правильного распознавания битов в каждой группе сигналов определяется произведением двух сомножителей:

– вероятностью правильного разделения принятого сигнала на две большие группы согласно формуле (4);

– условной вероятностью $C_n^m/2^n$ появления группы с числом переданных «1», равным m (C_n^m – количество сочетаний из m по n) [4].

В качестве примера рассчитаем вероятность правильного приема бита информации при параллельной передаче сигналов тремя линиями.

В кабеле из трех сигнальных линий возможны следующие группы сигналов:

$$\begin{gathered} S_{01}+S_{02}+S_{03};\ \sqrt{(E_1/2N_0)} = 0; \\ S_{11}+S_{02}+S_{03};\ S_{01}+S_{12}+S_{03};\ S_{01}+S_{02}+S_{13};\ \sqrt{(E_1/2N_0)} = x_1; \\ S_{11}+S_{12}+S_{03};\ S_{11}+S_{02}+S_{13};\ S_{01}+S_{12}+S_{13};\ \sqrt{(E_1/2N_0)} = 2x_1; \\ S_{11}+S_{12}+S_{13};\ \sqrt{(E_1/2N_0)} = 3x_1. \end{gathered} \tag{5}$$

где S_{0i} - сигнал низкого уровня в i-том канале («0»), его энергия $E_1 = 0$; S_{1i} - сигнал высокого уровня в i-том канале («1») с энергией E_1.

По уровню отношения $\sqrt{(E/2N_0)}$ сигналы крайних групп отличаются от порога на $1{,}5x_1$, поэтому вероятность их правильного приема определяется выражением

$$P_{0гр} = P_{3гр} = 0{,}5[(1+ \Phi(1{,}5x_1)]/8\ . \tag{6}$$

Сигналы двух средних групп отличается от порога на $0{,}5x_1$. Правильное распознавание уровня сигналов этих групп означает, что с вероятностью 2/3 во всех линиях передавались одинаковые сигналы (низкого или высокого уровня), а при неправильном распознавании вероятность уменьшается до значения 1/3, поскольку один бит из трех все же определяется правильно. Для сигналов средних групп вероятность правильного приема определяется выражением

$$P_{1гр} = P_{2гр} = \{0{,}5[(1+ \Phi(0{,}5x_1)](2/3)+ 0{,}5[(1 - \Phi(0{,}5x_1)](1/3)\}3/8 = [1{,}5+ 0{,}5\Phi(0{,}5x_1)]/8. \tag{7}$$

Для всех сигналов вероятность правильного приема бита переданной информации – это удвоенная сумма выражений (6) и (7)

$$P_1 = [4 + \Phi(0{,}5x_1) + \Phi(1{,}5x_1)]/8. \tag{8}$$

При малых значениях аргумента ($x_1 < 0{,}1$) значение функции Крампа пропорционально аргументу, поэтому выражение (8) можно представить в виде

$$P_3(x) \approx 0{,}5[1+ \Phi(x_1)] \tag{9}$$

Оно совпадает с выражением (4) для последовательной передачи. С увеличением значения аргумента x_1 вероятность правильного приема бита информации возрастает, но стремится не к 1, а к значению 0,75.

Аналогичный расчет для линии из восьми сигнальных проводов ($n = 8$) при значении порога $x_{пор} = 4x_1$ приводит к следующему выражению для определения вероятности P_8

$$P_8 = [128 + \Phi(4x_1) +6\Phi(3x_1) +7\Phi(2x_1) + 7\Phi(x_1)] / 256 \tag{10}$$

Зависимость вероятности правильного приема бита информации от аргумента x_1 для $n = 1$, $n = 3$ и $n = 8$ показана на рисунке.

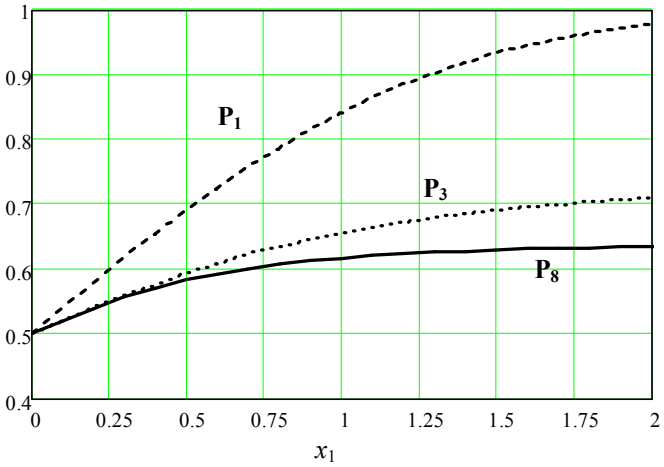

Рисунок – Зависимость вероятности правильного приема бита информации для последовательной передачи P_1 и параллельной P_3 ($n = 3$) и P_8 ($n = 8$) для оптимального приемника в зависимости от значения параметра x_1

Результаты расчетов предельного значения вероятности правильного приема бита информации $P_{мак}$ в зависимости от количества линий n, которые излучают одинаковые сигналы, приведены в таблице.

Таблица

n	2	3	4	5	6	7	8
$P_{мак}$	0,75	0,75	0,688	0,688	0,656	0,656	0,63

Оценим влияние неидентичности излученных сигналов на примере трех линий. Пусть излученный сигнал первой линией S_{11} отличается от сигналов остальных двух линий S_{12} и S_{13}. Энергию разностного сигнала обозначим ΔE_1, тогда отношение сигнал/шум для разностного сигнала $\Delta x_1 = \sqrt{(\Delta E_1/2N_0)}$. Если сигнал S_{11} отличается от остальных, то согласно (6) в первой и второй группе излученных сигналов слагаемые $S_{11}+S_{02}+S_{03}$ и $S_{01}+S_{12}+S_{13}$ отличаются от двух других слагаемых каждой группы. За счет этого для указанных суммарных сигналов вероятность правильного распознавания каждого из трех битов повышается от 2/3 при $\Delta x_1 = 0$ и до 1, если $\Delta x_1 > 3$. Остальные две пары суммарных сигналов между собой остаются неразличимыми, поэтому вероятность правильного распознавания каждого из трех переданных битов остается на уровне 2/3. В итоге, при большом отношении сигнал/шум ($x_1 > 3$) и безошибочном разделении суммарного сигнала на отдельные группы сигналы первой и третьей групп распознаются правильно, четыре суммарных сигнала первой и второй группы – правильно с вероятностью 2/3, а вероятность правильного распознавания остальных двух зависит от отношения сигнал/шум разностного сигнала Δx_1. Таким образом, для параллельной передачи трех сигналов, один из которых отличается от остальных двух, предельное значение правильного распознавания одного бита информации будет изменяется от 0,75 до 5/6.

При параллельной передаче n двоичных сигналов одной линией передается $1/n$ часть информации, поэтому влияние неидентичности одного сигнала можно рассчитать по приближенной формуле

$$P \approx P_n + (\Delta P_i - 0{,}5)/n\,, \qquad (11)$$

где P_n – вероятность правильного распознавания одинаковых двоичных сигналов, которая зависит от отношения сигнал/шум одного сигнала $x_1 = \sqrt{(E_1/2N_0)}$; ΔP_i – вероятность правильного распознавания разностного сигнала i-той линии, которая определяется выражением (4) для параметра $\Delta x_i = \sqrt{(\Delta E_i/2N_0)}$; ΔE_i – энергия разностного сигнала.

Сигналы параллельного кода обычно формируются одной микросхемой, поэтому параметры передаваемых импульсов (амплитуда, временная задержка, длительности фронтов и спадов) между собой отличаются незначительно. Практически одинаковы и характеристики излучения отдельных проводов многопроводного кабеля. Если принять, что энергия разностного сигнала не должна превышать десятой доли энергии сигнала, излученной одной линией, то для разностного сигнала отношение сигнал/шум не выходит за пределы $\Delta x_i < 0{,}32\sqrt{(E_1/2N_0)}$.

Обычно уровень побочного излучения достаточно мал и в точке возможного перехвата этого сигнала значение отношения сигнал/шум для одного сигнала $x_1 = \sqrt{(E_1/2N_0)} < 1$. При таких ограничениях отношение сигнал/шум для разностного сигнала $\Delta x_i < 0{,}32$, а расчетное значение превышения вероятности правильного приема бита информации согласно графической зависимости P_1 на рис. 1 не превышает значения $\Delta P_i < 0{,}07$ для одного *i*-того сигнала. Излученные сигналы других линий также могут отличаться между собой, но суммировать прирост вероятности каждого сигнала можно только для случая ортогональных (независимых) различий их параметров, например, один сигнал отличается от остальных по амплитуде, а второй - по задержке.

Для предельного случая, когда все сигналы отличаются между собой и условия ортогональности выполняются для всех разностных сигналов, с учетом множителя $1/n$ в выражении (11) суммарное превышение вероятности правильного распознавания бита информации не должно превышать значения $\Delta P < 0{,}07$ (при условии, что $x_1 < 1$). Поэтому с учетом поправки на возможный разброс излученных сигналов для параллельной передачи трех сигналов ($n = 3$) вероятность правильного распознавания бита информации не должна превышать значения $P < 0{,}72$.

Если сравнивать последовательную передачу (зависимость P_1 на рис. 1) и параллельную при $n = 3$, то при вероятности правильного распознавания бита информации $P = 0{,}72$ отношение сигнал/шум для последовательной передачи не должно превышать уровня $x_1 = 0{,}55$, в то время как для параллельной $x_1 = 1$. С увеличением числа параллельно передаваемых сигналов линией разница по допустимому отношению сигнал/шум только увеличивается. Согласно [2] считается, что при параллельной передаче сигналов восстановление передаваемой информации невозможно, если $n \geq 8$.

III Заключение

При параллельной передаче в пространство излучается суммарный сигнал, уровень которого пропорционален числу одновременно передаваемых импульсов. По уровню суммарного сигнала невозможно без ошибок определить линии, по которым передавался импульсный сигнал.

При малых соотношениях сигнал/шум ($x_1 < 0{,}1$) вероятность правильного приема бита информации для параллельной передачи чуть меньше вероятности последовательной передачи. Неоднозначность определения номера линии в этом случае компенсируется увеличением вероятности правильного распознавания суммарного сигнала на фоне шума за счет повышения среднего уровня суммарного сигнала по сравнению с уровнем сигнала в одной линии.

По мере увеличения отношения сигнал/шум различие между параллельной передачей и последовательной становится значимым. Неоднозначность распознавания номера линии, по которой передавался сигнал высокого уровня, приводит к обязательным ошибкам и ограничивает предельное значение вероятности правильного приема одного бита информации даже при больших отношениях сигнал/шум. Гарантированное наличие ошибок при приеме и распознавании сигналов побочного излучения при параллельной передаче можно рассматривать как определенный уровень защищенности такой передачи. Этот уровень повышается с увеличением числа одновременно передаваемых сигналов.

Список использованой Литературы: ***1*** *http://kiev-security.org.ua Побочные излучения и наводки.* ***2*** *Бузов Г. А., Калинин С. В., Кондратьев А. В. Защита от утечки информации по техническим каналам/ Учебное пособие, М.: Горячая линия-Телеком, 2005.* ***3*** *Помехоустойчивость и эффективность систем передачи информации/ А. Г. Зюко и др; Под ред. А. Г.Зюко.- М.: Радио и связь, 1985.-272с.* ***4*** *Бронштейн И. Н., Семендяев К. А. Справочник по математике для инженеров и учащихся ВТУЗОВ.*

Микола Романюков
ГУМВС України в Одеській області

УДК 621.373

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ SSD ТА HDD НАКОПИЧУВАЧІВ

Анотація: **Проведено огляд проблем виникнення електромагнітного випромінювання від засобів електронно-обчислювальної техніки та наведена порівняльна характеристика результатів вимірювання побічних електромагнітних випромінювань від SSD та HDD накопичувачів за допомогою комплексу АКОР-2ПК.**