УДК 621.396.67

МЕТОДИКА ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛОМ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ТА НАВЕДЕНЬ

Ю. І. Хлапонін**,** канд. техн. наук, старш. наук. співроб.

Національний авіаційний університет,

yfcnz0408@ukr.net

Останнім часом швидкий розвиток отримують методи перехоплення інформації каналами побічних випромінювань і наведень (ПЕМВН) елементів локальної мережі. Методика захисту окремих комп'ютерів добре опрацьовувана, затверджена необхідними нормативними документами. Проте завдання захисту інформації від витоку каналами ПЕМВН у локальній мережі істотно складніше, ніж для автономно використовуваних пристроїв. Тому для виявлення ПЕМВН сучасної електронно-обчислювальної техніки доводиться використовувати спеціальні організаційні, алгоритмічні та методичні підходи, які враховують ці проблеми. Проаналізовано методи пошуку сигналів ПЕМВН, які реалізовані в програмно-апаратних комплексах — метод різниці панорам, аудіовізуальний метод, експертний метод і параметрично-кореляційний метод. Метою роботи стала розробка методики оцінки захищеності інформації від витоку каналом ПЕМВН засобів електронно-обчислювальної техніки (ЕОТ) при використанні тестового сигналу у вигляді безперервної послідовності імпульсів. Наведено математичний апарат, який дозволяє вираховувати енергію одиночного сигналу при передачі логічної «1» або логічного «0». Наведені підходи можуть бути враховані при вдосконаленні методики проведення спеціальних досліджень ПЕМВН засобів ЕОТ.

Ключові слова: ПЕМВН, локальна мережа, захист інформації, оцінка захищеності, енергія сигналу, спектр сигналу, перетворення Фур'є.

Recently, methods of information interception with transient electromagnetic pulse emanation of local network elements are getting developed. Separate computers security methods are worked out well and backed up with necessary regulatory documents. However, information security through TEMPEST is far more hard to do in local network then in separate devices. That's why special institutional, algorithmic and methodological approaches should be used to detect electromagnetic pulse emanations. Methods of spotting TEMPEST were analyzed. There are panoramas difference method, audiovisual method, expert method and parametric correlation method. Development of methodology for assessing information security from the information outflow by the transient electromagnetic pulse emanation of computer technology by using the text signal as a continuous sequence of pulses was the main goal of this project The mathematical apparatus allows calculating the energy of a single signal by transfer logic "1" or a logical "0".These approaches can be considered into accounting by improving special researches of transient electromagnetic pulse emanation methods on EVT.

Keywords: transient electromagnetic pulse emanation, local network, data protection, protection rating, signal energy, signal spectrum, Fourier transformation.

Вступ

У зв'язку з бурхливим розвитком локальних і глобальних обчислювальних мереж широкий розвиток отримали методи розвідки (промислового шпигунства), спрямовані на перехоплення інформації, що обробляється (передається, зберігається) у локальних мережах. Як правило, проникнення в локальну мережу будь-якої організації можливо тільки за недостатньо кваліфікованого налаштування всіх елементів локальної мережі (включно і кожну робочу станцію) адміністратором системи. У разі ж якісного налаштування, застосування додаткових програмних і апаратних засобів, виконання необхідних організаційних заходів, шпигунам необхідно вишукувати методи добування інформації, не пов'язані з необхідністю проникнення в локальну мережу. Отже, останнім часом розвиток отримують методи перехоплення інформації каналами побічних випромінювань і наведень (ПЕМВН) елементів локальної мережі. Методика захисту окремих комп'ютерів досить добре опрацьована, підкріплена необхідними нормативними документами.

Завдання ж захисту інформації від витоку каналами ПЕМВН в локальній мережі істотно складніше, ніж для автономно використовуваних пристроїв.

Аналіз досліджень і публікацій

Сучасна техніка оброблення інформації характеризується низьким рівнем сигналів побічних електромагнітних випромінювань і наведень.

Низький рівень ПЕМВН є наслідком посилення санітарних норм, економії електроенергії для автономних і переносних пристроїв з батарейним живленням і збільшення швидкості обробки інформації до тих величин, зо яких стають істотними питання електромагнітної сумісності.

З іншого боку, якщо по провідниках передається змінний електричний струм зумовлений передачею інформації, то сигнали ПЕМВН обов'язково існують і їх необхідно виявити. Частотний діапазон побічних електромагнітних випромінювань, поширюється від одиниць кілогерц до ГГц і вище і визначається тактовою частотою використовуваного засобу обробки інформації.

Слід відзначити, що ПЕМВН утворюються від небезпечного сигналу. **Небезпечний (інформативний) сигнал** — сигнал, що містить, несе інформацію у відкритому вигляді [1].

Тому, для пошуку ПЕМВН сучасної техніки доводиться використовувати спеціальні організаційні, алгоритмічні та методичні підходи, які враховують дані проблеми.

Організаційні заходи полягають у створенні найкращих умов для випромінювання, поширення і прийому сигналів ПЕМВН. Для цього застосовуються такі підходи:

• розташування прийомної антени в безпосередній близькості від випромінюючих вузлів і блоків досліджуваної техніки;

• розпрямлення кабелів, по яких передається інформація для додання їм кращих антенних властивостей або розташування їх безпосередньо близько вимірювальної антени;

• заміна вимірювальної антени на струмозйомники і вимір несиметричного струму (того струму, який викликає електромагнітні випромінювання) в доступних провідниках, а потім на цих частотах пошук сигналів випромінювань за допомогою антен.

Природно, після проведення пошуку сигналів такими методами, вимірювання їх амплітуди необхідно проводити на коректній для вимірювання відстані. Якщо на попередньо знайдених частотах ПЕМВН на відстані вимірювання сигнал не виявляється, то випливає висновок про те, що на відстані вимірювання його амплітуда нижча за рівень індустріальних шумів.

Алгоритмічні та методичні підходи полягають у наступному. З розкладання періодичного сигналу (того сигналу, який утворюється тестовим режимом роботи устаткування) у ряд Фур'є випливає, що на частотах гармонік випромінюються немодульовані синусоїдальні сигнали (інформація або форма сигналу збирається зворотним розкладанням Фур'є з ряду сигналів на частотах гармонік). Нестабільність частоти такого сигналу визначається нестабільністю частоти опорного генератора. Задавальним генератором для цифрових сигналів, як правило — це кварц, що має нестабільність близько 5·10–5 Гц. Пошук і вимірювання сигналів ПЕМВН проводять за допомогою пікового детектора, який має дуже корисну для пошуку слабких сигналів властивість. Якщо смуга пропускання приладу повністю накриває сигнал, то амплітуда сигналу не змінюється за зміни смуги пропускання. Рівень шуму зменшується пропорційно кореню квадратному з зменшення смуги пропускання в кГц (наприклад при зменшенні смуги в 10 раз, шум зменшується більше ніж у 3 рази). Тому, точно налаштувавшись на сигнал гармоніки і зменшуючи смугу пропускання до тих величин, за яких смуга займаних частот сигналу не перевищує смугу пропускання вимірювального приладу, можна забезпечити максимальну чутливість вимірювального обладнання під час пошуку і вимірюванні сигналів ПЕМВН [2].

Методи виявлення сигналів ПЕМВН

Для пошуку сигналів ПЕМВН у програмно-апаратних комплексах можуть бути реалізовані такі методи — метод різниці панорам, аудіовізуальний метод, експертний метод і параметрично-кореляційний метод. Перші три методи є універсальними, тобто призначені для пошуку будь-яких сигналів ПЕМВН. Четвертий метод — параметрично-кореляційний метод призначений тільки для пошуку ПЕМВН відеосистеми комп'ютера (відеоадаптер-монітор), виключаючи цифрові канали передачі відеоданих (TFT матриці). Пошук ПЕМВН можна проводити як окремими методами, так і комбінувати їх у процесі роботи. Методи пошуку відрізняються один від одного за ступенем участі в них оператора. Повністю автоматичним методом є параметрично-кореляційний метод пошуку ПЕМВН моніторів. За ним, у міру автоматизації, слідує метод різниці панорам. Аудіовізуальний і експертний методи можна вважати автоматизованими методами. Беручи про увагу той факт, що робота ведеться зі слабкими сигналами, ідентифікувати які часто може тільки людина використовуючи свою інтуїцію і досвід, то за якістю одержуваних результатів методи пошуку можна розташувати в порядку зворотного ступеня автоматизації. Найкращі результати получають експертним методом. Хороші результати дає аудіовізуальний метод і замикає ряд метод порівняння панорам. Різниця в результати роботи проявляється в знаходженні слабких сигналів. Сигнали, які перевищують шум на 4–6 дБ усі методи знаходять стійко за умови правильно сформованого завдання на пошук сигналів. Параметрично-кореляційний метод дослідження моніторів дає дуже гарні результати за умови, що існує один або кілька добре помітних сигналів ПЕМВН, які метод використовують як базу для подальшого пошуку. Якщо таких сигналів немає, то метод може нічо-

го не знайти або прийняти невірні рішення. Оскільки у кожному разі відповідальність за проведену роботу несе оператор, результати роботи автоматичних методів необхідно контролювати.

Мета роботи — розробка методики оцінки захищеності інформації від витоку каналом ПЕМВН засобів ЕОТ при використанні тестового сигналу у вигляді безперервної послідовності імпульсів.

Після виявлення частот сигналів ПЕМВН необхідно коректно виміряти їх рівень. Під рівнем тут і далі розуміють пікове значення амплітуди сигналу. Необхідність уточнення рівнів сигналів викликане наступними міркуваннями.

1. Будь-який сигнал ПЕМВН має свою діаграму спрямованості і власний вектор поляризації. Тому, після виявлення сигналів ПЕМВН необхідно перевиміряти їх рівень, налаштувавшись на максимальний пелюсток діаграми спрямованості і знайти правильний вектор поляризації. На рис. 1. наведено отриманий експериментально вигляд діаграми спрямованості ПЕМВН системного блоку комп'ютеру в корпусі, який серійно випускається [3].

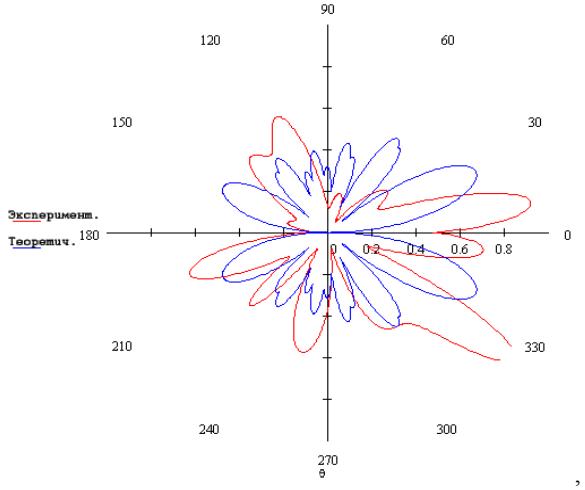

Рис. 1. Діаграма спрямованості ПЕМВН серійного комп'ютера

2. Слабкі сигнали ПЕМВН, як правило, сильно модульовані шумом. Виражається це в істотній зміні рівня сигналу під час його вимірювання. На сьогодні існує єдиний метод експертної оцінки рівня перешкоди сигналу по картинці продетектованного і розгорнутого у часі радіосигналу (режим нульового огляду аналізатора спектра або осцилографічний режим). Такий експертний аналіз рівня зашумленного сигналу має місце при експертному методі.

Далі на прикладі визначення ймовірності перехоплення сигналу розглянемо методику оцінки захищеності кабельної лінії, по якій передається інформативний сигнал.

Інформативні сигнали, використовувані при передачі інформації між елементами автоматизованої системи подаються імпульсами: логічна «1» і логічний «0». При цьому існує два види кодування інформації: імпульсне і кодування. При імпульсному кодуванні логічна «1» передається прямокутним імпульсом, а логічний «0» — відсутністю імпульсу.

Імовірність виявлення сигналу на фоні адитивного білого гауссового шуму не залежить від форми сигналу або ширини спектру сигналу, а визначається тільки відношенням енергії сигналу в точці прийому до спектральної щільності шуму:

$$q = \sqrt{\frac{\mathrm{E_c}}{N_0}},$$

де q — відношення пікової напруги сигналу до середньоквадратичного значення шуму на виході оптимального приймача; $\mathrm{E_c}$ — енергія прийнятого сигналу; N_0 — спектральна щільність шуму.

Енергія сигналу в загальному випадку дорівнює інтегралу від потужності по всьому проміжку існування сигналу,

$$\mathrm{E_c} = \int_{-\infty}^{\infty} p(t)dt = \int_{-\infty}^{\infty} |u(t)|^2 \, dt,$$

де $\mathrm{E_c}$ — повна енергія сигналу; $p(t)$ — миттєва потужність сигналу; $u(t)$ — миттєве значення напруги сигналу.

Згідно з теоремою Парсеваля, енергія сигналу може бути обчислена за його спектрального представлення,

$$\mathrm{E_c} = \int_{-\infty}^{\infty} |G(f)|^2 \, df \quad \text{або} \quad \mathrm{E_c} = \int_{-\infty}^{\infty} E(f)^2 df, \qquad (1)$$

де $G(f)$ — амплітудно-частотний спектр сигналу; $E(f)$ — напруженість електричного поля інформативного сигналу на частоті f.

У реальних умовах неможливий вимір миттєвих значень потужності або напруги інформативного сигналу, випроміненого в простір. Тому енергію необхідно визначати за формулою (1) після оцінки рівнів спектральних складових вузькосмуговим приймачем.

Незважаючи на уявну простоту виразу, визначення енергетичних характеристик, на практиці зустрічаються певні труднощі. Основний вплив роблять власні шуми приймального пристрою, який застосовується як вузькосмуговий приймач для оцінки спектра інформативного сигналу. Справа в тому, що енергетичний спектр реальних сигналів є суцільним. Так, наприклад, якщо при передачі інформації використовується імпульсне кодування, причому логічна «1» подаються імпульсом тривалістю τ, то спектр кожного такого імпульсу має вигляд $\sin(x)/x$ (рис. 2).

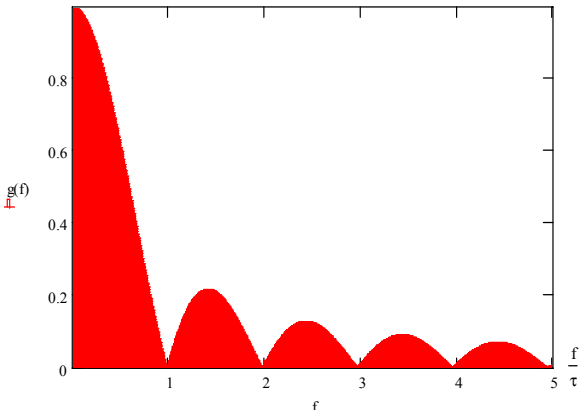

Рис. 2. Спектр імпульсів тривалістю τ при імпульсному кодуванні

Для сигналів з безперервним спектром напруга на виході широкосмугового приймача $\left(\Delta F_{\text{пр}} \le \frac{1}{\tau_u}\right)$ амплітуда вихідної напруги залежить від смуги пропускання цього приймача.

Для зменшення власних шумів прагнуть зменшити смугу пропускання приймача, однак при цьому зменшується і потужність сигналу. Таким чином, отримати прийнятне співвідношення сигнал/шум у процесі експериментальної оцінки спектра досить важко. Проте в процесі оцінювання спектра можна підібрати спеціальний тестовий сигнал, при передачі якого спектр випромінюваного сигналу стає лінійчатим.

Таким сигналом, зокрема, може бути безперервна послідовність імпульсів (чергування логічних «1» і «0») з наперед визначеною частотою повторення $F_{\text{п}}$. Спектр безперервної лінійчатої послідовності імпульсів показано на рис. 3.

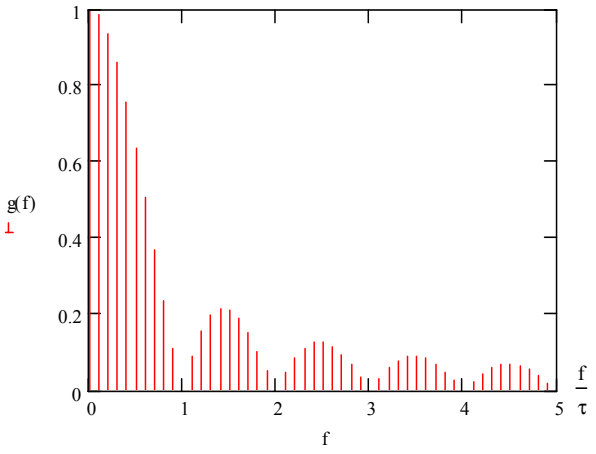

Рис. 3. Спектр безперервної послідовності імпульсів

Для сигналу з лінійчатим спектром можна як завгодно зменшити смугу пропускання вимірювального приймача, при цьому потужність власних шумів приймача зменшуватиметься пропорційно зменшенню смуги пропускання без зміни потужності спектральної складової інформативного сигналу, що потрапляє в смугу пропускання приймача. Однак, тестовий сигнал неадекватний реальному. Тому, якщо вимірювання напруженості поля інформативного сигналу проводиться за тестовим сигналом, то для визначення співвідношення сигнал/шум, яке можливе для реальної ситуації, необхідно перерахувати отримані значення з урахуванням різниці в спектрах реальних сигналів і тестового сигналу. Сутність перерахунку полягає в такому. Вважається, що для перехоплення інформації необхідно і достатньо правильно прийняти кожен імпульс, що представляє логічна «1». Таким чином, завдання перехоплення інформації зводиться до завдання виявлення із заданою вірогідністю одиночного імпульсу з відомими параметрами. Спектр реально перехоплюваного сигналу (а, отже, і частотна характеристика оптимального для перехоплення приймача) відповідає рис. 2. Спектр же тестової періодичної послідовності імпульсів, що представляють логічну «1», відповідає рис. 3. На частотах, кратних частоті повторення імпульсів $F_{\text{п}}$ комплексні амплітуди ряду Фур'є спектру періодичної послідовності імпульсів довільної форми вирізняються від значень спектральної щільності амплітуд одиночного імпульсу в цих точках рівно в $F_{\text{п}}$ разів:

$$\frac{\dot{A}_n}{2} = \frac{1}{T_{\text{п}}} G(n\omega_0) = F_{\text{п}} G(n\omega_0),$$

де $\frac{\dot{A}_n}{2}$ — комплексна амплітуда ряду Фур'є; $F_{\text{п}} = \frac{1}{T_{\text{п}}}$ — частота повторення імпульсів; $\omega_0 = 2\pi F_{\text{п}}$ — кругова частота повторення імпульсів; $G(n\omega_0)$ — значення спектральної щільності амплітуд одиничного імпульсу на частоті $\omega = n\omega_0$.

Інакше кажучи, замість оцінки спектра випромінюваного інформативного сигналу при використанні тестового сигналу у вигляді періодичної послідовності імпульсів, отримуємо значення напруженості поля тільки на частотах $nF_{\text{п}}$, які до того ж відрізняються від шуканих значень спектральної щільності амплітуд реального сигналу в цих точках у $F_{\text{п}}$ разів.

Щоб за виміряним значенням отримати енергію випромінюваного інформативного сигналу, замінимо інтеграл у виразі (1) сумою інтегралів:

$$\text{E}_{\text{c}} = \int_0^{F_{\text{п}}} E(f)^2 df + \int_{F_{\text{п}}}^{2F_{\text{п}}} E(f)^2 df + \cdots.$$

Кожен інтеграл наведеної вище суми може бути наближено обчислений як добуток інтерва-

лу інтегрування (у даному випадку $F_{\text{п}}$) на значення підінтегрального виразу в точках $f = F_{\text{п}}, 2F_{\text{п}}, ..., nF_{\text{п}}$: $\text{E}_{\text{с}} = F_{\text{п}} \sum_n E^2(nF_{\text{п}})$.

Враховуючи, що $E(nF_{\text{п}}) = \text{E}_{F_{\text{п}}}^{\text{изм}}$, отримуємо в результаті:

$$\text{E}_{\text{с}} = F_{\text{п}} \sum \left(\frac{E_n^{\text{изм}}}{F_{\text{п}}} \right)^2 = \frac{\sum_n \left(E_n^{\text{изм}} \right)^2}{F_{\text{п}}},$$

або

$$\sqrt{\text{E}_{\text{с}}} = \frac{\sqrt{\sum_n \left(E_n^{\text{изм}} \right)^2}}{\sqrt{F_{\text{п}}}}. \qquad (2)$$

Саме вираз (2) лежить в основі пропонованої методики оцінки захищеності при використанні тестового сигналу у вигляді безперервної послідовності імпульсів.

У випадку, коли логічна «1» і логічний «0» представлені різними сигналами, а не наявністю і відсутністю прямокутного імпульсу, енергія сигналу повинна визначатися за загальним виразом:

$$\text{E}_{\text{с}} = \int \left[E_1(t) - E_0(t) \right]^2 dt, \qquad (3)$$

де $E_1(t)$ і $E_0(t)$ — напруженість електричного поля при передачі логічної «1» і логічного «0» відповідно.

У більшості практичних випадків вираз (3) можна істотно спростити. Розкриваючи в даному виразі дужки, отримаємо:

$$\text{E}_{\text{с}} = \int_{-\infty}^{\infty} E_1^2(t)dt - 2\int_{-\infty}^{\infty} E_1(t)E_0(t)dt + \int_{-\infty}^{\infty} E_0^2(t)dt. \quad (4)$$

Якщо енергія сигналу під час передачі логічної «1» дорівнює енергії сигналу при передачі логічного «0», тобто, $E_1 = E_0 = E$, то вираз (4) легко перетвориться до вигляду:

$$\text{E}_{\text{с}} = 2\text{E}_{1,0} \left(1 - \frac{\int_{-\infty}^{\infty} E_1(t)E_0(t)dt}{\int_{-\infty}^{\infty} E_1^2(t)dt \int_{-\infty}^{\infty} E_0^2(t)dt} \right),$$

де $\text{E}_{1,0}$ — енергія одиночного сигналу при передачі логічної «1» або логічного «0».

Другий доданок у дужках це — коефіцієнт кореляції сигналів ρ.

З урахуванням цього отримуємо остаточний вираз, еквівалентний (4), але більш зручний для практичного застосування.

$$\text{E}_{\text{с}} = 2\text{E}_{1,0}(1 - \rho).$$

Значення ж $\text{E}_{1,0}$ можна отримати за виразом (2).

Для пошуку сигналів ПЕМВН проводять два вимірювання рівнів електромагнітного поля біля досліджуваного об'єкта — перший раз за вимкненого тестового сигналу, другий — за ввімкненого тестового сигналу. Далі відбувається віднімання графіка рівнів електромагнітного поля виміряного за вимкненого тестового сигналу з графіка рівнів електромагнітного поля виміряного при включеному тестовому сигналі. Зареєстровані частотні точки, у яких сигнали з другого графіка перевищили сигнали з першого графіка на заздалегідь визначений оператором поріг потрапляють у список частот імовірних сигналів ПЕМВН.

Висновок

У цій статті розглянуто особливості виникнення каналу витоку інформації за рахунок побічного електромагнітного випромінювання, наведено та запропоновано методику оцінки захищеності інформації від витоку каналом ПЕМВН засобів ЕОТ (кабельної лінії локальної мережі) при використанні тестового сигналу у вигляді безперервної послідовності імпульсів.

Наведені підходи можуть бути враховані при вдосконаленні методики проведення спеціальних досліджень ПЕМВН засобів ЕОТ.

ЛІТЕРАТУРА

1. *Ленков С. В.* Методы и средства защиты информации / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко; под ред. В. А. Хорошко. — К. : Арий, 2010. — Т. I. Несанкционированное получение информации. — 464 с.

2. *Пятачков А. Г.* Защита информации, обрабатываемой вычислительной техникой, от утечки по техническим каналам / А. Г. Пятачков. — М. : НП РЦИБ «Факел», 2007.

3. [Електронний ресурс]. — Режим доступу: http://www.epos.ua/view.php/about_pubs_archive?subaction=showfull&id=1037743200&archive=%20&start_from=%20&ucat=2&

Стаття надійшла до редакції 24.11.2015