5 Короткі повідомлення

ЗАХИСТ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД ЕЛЕКТРОМАГНІТНОГО ТЕРОРИЗМУ, ІНДУСТРІАЛЬНИХ ЗАВАД ТА НЕСАНКЦІОНОВАНОГО ЗЙОМУ ІНФОРМАЦІЇ ПО ЕЛЕКТРОМЕРЕЖІ

Володимир Павловський
Фірма ЕМСБІ

Анотація: **Описано проблематику захисту комп'ютерних систем від витоку інформації по електромережі, електромагнітного тероризму та індустріальних завад з електромережі.**
Summary: **This article is about protection of computer systems from information leakage via power line, electromagnetic terrorism and industrial power line interference.**
Ключові слова: **Технічний захист інформації, електромережні фільтри, електромагнітний тероризм, захист інформації від витоку, ПЕМІН.**

I Проблема витоку інформації з комп'ютерів та іншої офісної техніки

Для складних інформаційних систем цифрової та/або аналогової обробки сигналів (комп'ютери, офісні АТС, модеми, принтери тощо) вже стала традиційною і не втрачає актуальності проблема захисту від несанкціонованого доступу та зйому інформації. Джерелами витоку інформації є мережі електроживлення, пожежної та охоронної сигналізації, факс-модемні лінії тощо. Будь-який провідник у кімнаті з увімкненим комп'ютером або іншою електронною технікою працює як антена: приймає електромагнітні сигнали, що випромінює електронна техніка і передає їх назовні. Зацікавлена у ваших секретах сторона може за допомогою спецтехніки прочитати і розшифрувати ці сигнали.

Сучасні інформаційні системи працюють на тактових частотах вище 2 ГГц. При таких тактових частотах вищі гармоніки центрального процесора сягають частот 10 ГГц і вище. Це означає, що інформація може витікати з системи на частотах до 10 ГГц як по ефіру, шляхом радіовипромінювання, так і по проводах мережі електроживлення. Захист від витоку інформації по ефіру шляхом екранування кімнат, де розташована техніка, навіть екранування самої техніки вирішує лише частину проблеми. Доки не припинено витік інформації по електромережі, ваші секрети залишатимуться вразливими до промислового та інших видів шпіонажу.

Більшість електромережних фільтрів для захищеної техніки гарантують припинення витоку інформації по проводах мережі електроживлення на частотах до 1 ГГц, залишаючи діапазон 1-10 ГГц "неприкритим". Майбутнє галузі ТЗІ в Україні – за фільтрами, що ефективно протидіють витоку інформації в діапазоні вище 1 ГГц, зменшуючи випромінювані в мережу сигнали до рівнів, на яких їх неможливо прочитати та розшифрувати.

II Проблеми "брудної" електромережі. НСД або електромагнітний тероризм. Захист електронної техніки електромережними фільтрами

Низька якість електроенергії в мережі електроживлення є очевидним фактом. В мережі реєструють величезну кількість коротких сплесків перенапруги з амплітудою в сотні вольт, а також одиничні імпульси з амплітудами до декількох кВ. Ці імпульси виникають через те, що в мережі електроживлення працюють потужні промислові установки, зварювальне обладнання, до неї під'єднаний міський електротранспорт, високочастотне промислове та медичне обладнання. Інколи в мережі трапляються аварійні замикання; вони теж спричиняють виникнення сплесків перенапруги. Крім того, грозова активність навесні та влітку, удари блискавки поблизу підстанцій породжують в мережі перенапруги ще більшої амплітуди та енергії. Не менш важливою є задача захисту електронного обладнання від збоїв та виведення з ладу навмисною силовою дією (НСД) по мережі електроживлення. Для НСД або так званого «електромагнітного тероризму» використовують спеціальні технічні засоби, що під'єднуються до мережі за допомогою гальванічного зв'язку, через конденсатор або трансформатор. Озброєний цією технікою терорист може створити різкий сплеск перенапруги в мережі живлення комп'ютера або іншої системи обробки інформації. Амплітуда, тривалість та енергія створеного сплеска такі, що здатні спричинити збій в роботі системи, втрату інформації

і навіть вихід з ладу апаратної частини. Сьогодні у світі кількість випадків крадіжки інформації неухильно зростає, комп'ютерні злочини стають дедалі витонченішими, не кажучи вже про так звану "електромагнітну зброю", що розробляється і, за деякими даними, вже застосовується в певних країнах. Традиційних засобів (UPS та ін.) не тільки недостатньо для захисту від НСД – вони самі можуть бути знищені НСД. З наведених фактів постає тривожна тенденція для всіх, хто хоче зберегти та захистити свою інформацію: більшість комп'ютерів та інших електронних носіїв інформації беззахисні перед можливою "електромагнітною атакою", так само, як і перед згаданими вище сплесками перенапруги в мережі від природних явищ або від аварій в мережі.

Перспективним напрямом для замовників та розробників техніки для галузі ТЗІ є впровадження фільтрів, що ефективно захищають згадані засоби обробки інформації від "брудної" електромережі, від дії високовольтних імпульсних завад тривалістю 10...50 мкс та від дії пачок високовольтних імпульсних завад наносекундного діапазону, які можуть поступати з мережі електроживлення.

III Проблема електробезпеки при живленні комп'ютерів від електромережі. Струм витоку електромережних фільтрів як мірило їх електробезпеки для людини

До фільтрів, під'єднаних до електромережного входу комп'ютера, висувають особливі вимоги щодо електробезпеки. Це пов'язано з тим, що комп'ютери належать до класу радіоелектронних пристроїв з неконтрольованим заземленням.

Мірилом безпеки фільтра є так званий струм витоку. Цей показник жорстко регламентується вітчизняними та міжнародними стандартами. Фільтр зі струмом витоку більше 20...30 мА, під'єднаний до комп'ютера, може перетворитися на замаскованого електричного стільця при обриві або відсутності заземлення.

Проблем не виникає, якщо у фільтрі для комп'ютера струм витоку не перевищує 3,5 мА.

Електромережний фільтр має бути безпечним в експлуатації навіть при обриві або відсутності заземлення, а також повністю відповідати вимогам вітчизняного стандарту ДСТУ 3639 – 97 "ФІЛЬТРИ ПРОТИЗАВАДНІ" та стандарту ГОСТ 25861 "Машины вычислительные и системы обработки данных. Требования электрической и механической безопасности и методы испытаний".

IV Встановлення та під'єднання електромережних фільтрів

Показники будь-яких фільтрів можуть бути повною мірою реалізовані лише за умови правильного з точки зору високочастотної техніки встановлення фільтра на місце експлуатації та під'єднання його до споживача і мережі.

Коливання високої та надвисокої частоти дуже легко "просочуються" крізь нещільний екран або в обхід неправильного встановленого екрану. Неправильне з'єднання фільтра з заземленням з точки зору високочастотної техніки також може звести нанівець загасання, яке він вносить.

Бажано, щоб виробник конкретного типу електромережних фільтрів виробляв спеціальні кріплення під вимоги конкретного замовника, та надавав послуги зі встановлення та під'єднання фільтра на місці експлуатації у замовника, а також періодичної перевірки роботоспроможності фільтрів під час експлуатації.

Компактні (трохи більші за звичайний мережевий адаптер), легкі (менше 1,5 кг), зроблені з урахуванням підвищених вимог з електробезпеки, з розширеним діапазоном захисту інформації від витоку та з функцією захисту від імпульсних завад – саме такі фільтри назвуть фільтрами нового покоління, адже за своїми технічними характеристиками вони цілком відповідають міжнародному рівню в галузі ТЗІ по електромережі.

*Література: **1**. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. Москва, Радио и Связь, 2001. **2**. Торокин А. А. Основы инженерно-технической защиты информации. Москва, Издательство «Ось-89», 1998. **3**. Хорев А. А. Способы и средства защиты информации. Москва, МО РФ, 2000. **4**. Сухоруков С. А. Защита электронного оборудования от помех в сетях электропитания. Журнал «Конфидент», №4, 1998, с. 23-29 **5**. Сухоруков С. А. Защита информационно-вычислительных систем от намеренного силового воздействия по коммуникационным каналам. Журнал «Конфидент» №2, 1998, с. 42-47.*