2 Соответствующим подразделениям СБУ, совместно с министерствами, ведомствами, ведущими предприятиями, организациями, НИИ, КБ Украины необходимо провести работу по разработке Концепций защиты наиболее важных объектов.

Литература: *1. Закон Украины "О государственной тайне". 2. Свод сведений, составляющих государственную тайну Украины. 3. Правове, нормативне, та метрологічне забезпечення систем захисту інформації в Україні// Матеріали ювілейної науково-технічної конференції. - Київ, 1998. 4. Указ Президента РФ № 212 от 19.02.99г. "Положение о Государственной технической комиссии при Президенте Российской Федерации". 5. Каторгин Ю.Ф. и др. Энциклопедия промышленного шпионажа. - С.-Петербург: Полигон, 1999. 6. Концепция технической защиты информации в Украине. 7. Методические рекомендации государственным экспертам по вопросам тайн по определению оснований для отнесения сведений к государственной тайне и степени их секретности.*

УДК 621.96

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЕОМ ДЛЯ ОБРОБКИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В СУЧАСНИХ УМОВАХ

Георгій Левченко, Михайло Ільченко, Володимир Хорошко, Валерій Буркацький, Костянтин Золотухін, Володимир Грошев

Науково-виробниче підприємство "Плазмотехніка", Національний технічний університет України "КПІ", Київський міжнародний університет цивільної авіації, Генеральний штаб Збройних Сил України, Державний упроваджувальний центр "Спецтехніка" МВС України

Анотація. **Розглянуто проблеми захисту інформації від витоку по ПЕМВН та електромагнітного тероризму. Проаналізовані особливості застосування екранованих приміщень та генераторів шуму. Запропоновані організаційні заходи щодо підвищення рівня інформаційної безпеки державних органів та критичних інфраструктур з використанням ЕОМ в захищеному виконанні за ГОСТ29339. Сформульовані пропозиції можуть бути використані банками та іншими небайдужими до захисту інформації організаціями.**

Summary. **Problems of protection of information from leakage by electromagnetic emanation and from electromagnetic terrorism are considered. Features of application of shielded premises and generators of a noise are analyzed. Organizational measures on rise of a level of information safety of state bodies and critical infrastructures with use of computers in protected fulfillment by GOST29339 are offered. Use of suggestions by banks and other not indifferent to protection of the information organizations is possible.**

Ключові слова: **захист, інформація, екранування, випромінювання, норми.**

Впровадження в усі сфери життєдіяльності держави інформаційних технологій зумовило розширення сфери застосування ЕОМ для обробки інформації з обмеженим доступом (ІзОД). Така інформація в наш час потребує додаткового підвищення ступеня захищеності як від перехоплення її по побічних електромагнітних випромінюваннях та наводах (ПЕМВН), так і від навмисного силового електромагнітного впливу, який може спотворити її або зовсім знищити.

Завдяки науково-технічному прогресу сучасні засоби перехоплення інформації якісно відрізняються від тих, на які орієнтована чинна нормативна база в галузі технічного захисту інформації. Так, сучасна портативна апаратура перехоплення своїми можливостями відповідає стаціонарній 70-х років, а за деякими характеристиками перевищує останню.

Цифрова обчислювальна техніка дозволяє реалізувати оптимальний прийом та забезпечити накопичення будь-якої достатньої кількості повторів для відновлення перехопленої інформації не апаратними засобами, як раніше у стаціонарних комплексах радіо- та радіотехнічної розвідки, а на рівні програмного забезпечення.

Значне покращення характеристик радіоприймальних пристроїв (зокрема, зниження рівня власних шумів, підвищення чутливості, різке зменшення габаритів і маси) і використання малогабаритних ЕОМ з відповідним програмним забезпеченням дозволяють створити портативні системи з реалізацією на одній і тій самій апаратній

базі (навіть одночасно) кількох оптимальних приймачів з різними алгоритмами обробки сигналів, в тому числі адаптивними.

Крім того, істотне зменшення розмірів антенних систем з підвищенням робочої частоти, зростання тактових частот ЕОМ та застосування високоефективних направлених, зокрема активних, антен також значно полегшують реалізацію портативних систем перехоплення. Такі системи можуть бути розміщені в "дипломаті", що дозволяє на мінімальній відстані до об'єкта проводити як перехоплення інформативних сигналів з повним відновленням інформації в режимі реального часу, так і запис (можливо і безперервно - до кількох тижнів) та збереження перехоплених сигналів для подальшої обробки в стаціонарних комплексах.

Так, наприклад, портативний програмно-апаратний комплекс 4625-COM-INT (габарит 25х53х35 см, маса 18 кг, діапазон частот 25-2000 МГц, чутливість 0,15 мкВ) відновлює перехоплену інформацію у тому самому вигляді, що відображався на екрані ЕОМ [4,5].

Необхідно також зазначити, що витрати, безпосередньо пов'язані з перехопленням і відновленням інформації, не залежать від ступеню секретності оброблюваної інформації.

Окремо слід підкреслити важливість проблеми електромагнітного тероризму, тобто уразливості ЕОМ до навмисного силового впливу електромагнітним випромінюванням.

За допомогою потужних електромагнітних випромінювань можна спотворити або зовсім знищити інформацію та вивести з ладу ЕОМ, які її обробляють. Це може дезорганізувати роботу, порушити надійність і стійкість управління об'єктами або навіть цілими регіонами країни. На відміну від ядерного, хімічного або біологічного тероризму такі акції не потребують проникнення на об'єкт і можуть здійснюватися дистанційно, з-за меж контрольованої зони.

Зростаючу стурбованість щодо загрози електромагнітного тероризму виявляє Міжнародна електротехнічна комісія. В США проведені спеціальні слухання в Конгресі з цієї проблеми, і створено Національний центр захисту інфраструктури, на який покладено завдання забезпечення всебічного захисту комп'ютерних систем, із зростанням обсягів його фінансування до 1 млрд. доларів у 2004 р. Аналогічні заходи вживаються в Європі, Японії, Китаї [3].

За результатами досліджень дії потужних електромагнітних випромінювань на комп'ютерні і телекомунікаційні центри та інші об'єкти створено прототипи радіопроменевої зброї, що були застосовані США під час бойових дій в Перській затоці та Югославії.

Малогабаритні генератори потужних надширокополосних електромагнітних випромінювань можуть мати масу близько 25 кг, бути розміщені в чемодані середніх розмірів та застосовані в безпосередній близькості до об'єктів [3].

Отже, як засоби перехоплення інформації, так і згадані засоби електромагнітного нападу можуть мати досить малі габарити та бути приховані, зокрема, в транспортних засобах або неконтрольованих "дипломатах". Вони можуть знаходитися практично впритул до об'єктів ЕОТ впродовж всього робочого часу, коли саме і здійснюється оброблення більшої частини обсягів ІзОД. При цьому потребу в отриманні інформації та можливість придбання необхідної апаратури можуть мати не тільки іноземні спецслужби, а й будь-які інші зацікавлені організації чи особи (для закладів МВС, СБУ, прокуратури, податкових адміністрацій, банків тощо - наприклад, представники криміналу).

На підставі вищевикладеного обгрунтування та для забезпечення необхідного в наш час рівня захищеності ІзОД від витоку по ПЕМВН та навмисного силового електромагнітного впливу, об'єкти вищих державних органів, силових та правоохоронних відомств, окремих центральних органів виконавчої влади та критичних інфраструктур слід, на нашу думку, вважати розміщеними в, так би мовити, "надзвичайних умовах розташування" з точки зору захисту інформації.

Слід підкреслити, що цей підхід відповідає вимогам щодо визначення ступеня захищеності засобів і об'єктів ЕОТ від витоку інформації за рахунок ПЕМВН, встановленим нормативним документом 1981 р. для об'єктів ЕОТ.

Крім того, для забезпечення достатнього рівня захищеності ІзОД оброблення такої інформації повинно здійснюватися лише ЕОМ в захищеному виконанні, які відповідають вимогам чинного в Україні ГОСТ 29339-92, на жаль, недостатньо поширеного серед фахівців.

Слід відрізняти термін "ЕОМ в захищеному виконанні" (за термінологією ГОСТ 29339-92 – по ПЕМВН) від виразу "захищена ЕОМ" (додатковими засобами, наприклад, від НСД, просторовим зашумленням або екрануванням приміщення).

ЕОМ в захищеному виконанні за ГОСТ 29339-92 забезпечує надійний захист оброблюваної інформації від витоку її по ПЕМВН, навмисного силового впливу по ефіру та від апаратних закладок. В той же час використання систем просторового зашумлення лише частково вирішує проблему захисту інформації тільки від перехоплення по ПЕМВН, не захищаючи зовсім від навмисного силового впливу та апаратних закладок.

Системи просторового зашумлення додатково підвищують рівень електромагнітного випромінювання, створюють завади для РЕА, демаскують місцезнаходження об'єкта та час оброблення ІзОД. Крім того, не виключена можливість зменшення чи ліквідації зовсім захисної дії генератора шуму, наприклад, просторовою

селекцією направленими антенами та сучасними методами обробки сигналів. Задача виділення інформативного сигналу із суміші сигнал/завада може бути значно полегшена за умови попереднього визначення характеристик інформативних сигналів ЕОМ, перехоплених з демаскованого об'єкта в період відсутності просторового зашумлення. Слід також зауважити, що характеристики випромінювання інформативних сигналів не залежать від ступеню секретності оброблюваної інформації.

Діапазон робочих частот генераторів шуму, які пропонуються для маскування інформативних випромінювань, не перевищує 1 ГГц, а витік інформації можливий і на більш високих частотах (до 10-15 гармоніки тактової частоти, що на сьогодні значно перевищує 1 ГГц). Сучасні ж портативні автоматизовані засоби забезпечують перехоплення сигналів частотою до 30 ГГц [1, 2, 5, 6].

До того ж робота генераторів шуму, завдяки їх досить значній інтегральній потужності та широкому частотному діапазону випромінювання, м'яко кажучи, відбивається на самопочутті персоналу і не залишається непоміченою ним, тому найчастіше під час обробки ІзОД ці генератори взагалі "забувають" вмикати. Таким чином, витрати на придбання генераторів шуму з метою захисту інформації в ЕОМ зрештою можуть виявитися марними.

Застосування екранованих приміщень є досить ефективним засобом захисту ЕОМ, особливо при використанні подвійного чи навіть потрійного екранування, проте має і ряд недоліків.

По-перше, це дуже висока вартість спорудження екранованих приміщень, особливо при необхідності забезпечення високого ступеня екранування, та значні поточні витрати на підтримання відповідного рівня захисту.

По-друге, екроване приміщення створює дискомфортні умови для працюючих в ньому. У випадку розміщення в одному екранованому приміщенні кількох ЕОМ умови праці погіршуються ще більше внаслідок відбивання та складання випромінювань від окремих ЕОМ. Це добре знають усі, кому довгий час доводилось працювати в екранованих приміщеннях.

В той же час є повідомлення про перехоплення і повне відновлення інформації на відстані 20 м з монітора ЕОМ, розташованої в екранованому приміщенні [1, 6].

Слід згадати ще один метод захисту ЕОМ, що інколи застосовується на практиці, - метод підбору комплектації ЕОМ за мінімальними рівнями випромінювань. Він дозволяє дещо знизити рівні ПЕМВН конкретного екземпляру ЕОМ, проте повністю виключає взаємозамінність складових частин, наприклад, в разі необхідності ремонту, і є прямим порушенням вимог ГОСТ 23773-88, згідно з яким спеціальний відбір комплектуючих елементів за технічними параметрами для ЕОМ не дозволяється.

ЕОМ загального призначення в захищеному виконанні в процесі приймальних випробувань обов'язково повинні проходити спецдослідження на відповідність вимогам ГОСТ 29339-92.

До складу конструкторської документації на ЕОМ в захищеному виконанні повинен входити і надаватися виробником до кожного екземпляру ЕОМ «Припис на експлуатацію ЕОМ в захищеному виконанні» (надалі – «Припис»). Припис є основним керівним документом з захисту саме ЕОМ, його наявність та зміст передбачені чинними нормативними документами.

Враховуючи значну залежність ефективності захисту інформації від фактичного ступеня захищеності ЕОМ, на нашу думку, слід вносити їх (ЕОМ) до Переліку засобів загального призначення, дозволених для використання з метою ТЗІ, виключно за результатами спецдосліджень, проведених ДСТСЗІ СБ України на відповідність вимогам ГОСТ 29339-92.

Згідно з ГОСТ 29339-92 вимоги до захисту складових частин засобів обчислювальної техніки повинні відповідати вимогам до захисту ЕОМ в цілому, тому спецдослідження персональних комп'ютерів (робочих станцій) та серверів в захищеному виконанні слід проводити у комплекті з моніторами, клавіатурами, маніпуляторами «миша», кабелями тощо.

Мережні протизавадні фільтри, що призначені для використання у складі ЕОМ в захищеному виконанні з метою запобігання витоку оброблюваної інформації колами електроживлення, додатково до випробувань на відповідність вимогам з внесеного загасання та електробезпеки повинні також проходити випробування на відсутність електроакустичних перетворень (на вимогу замовника) та обов'язково спецдослідження на відповідність вимогам ГОСТ 29339-92.

ЕОМ характеризуються рівнями ПЕМВН, за вимірюваннями яких визначають зону можливого перехоплення інформації (зону 2), і не повинні підлягати категоруванню.

Категоруванню повинні підлягати об'єкти обчислювальної техніки, тобто ЕОМ разом з приміщеннями, в яких вони розміщені. Об'єкти характеризуються контрольованими зонами (організаційними заходами).

ЕОМ можуть бути в захищеному чи в не захищеному виконанні, що залежить від того - відповідають чи не відповідають їх параметри вимогам ГОСТ 29339-92 в цілому, тому вираз "ЕОМ II категорії" взагалі не визначає ступеня захищеності ЕОМ від витоку інформації по ПЕМВН.

Слід зазначити, що криптографічні засоби забезпечують захист інформації лише за умови виключення можливості перехоплення інформації по ПЕМВН, зокрема, під час її виводу на кінцеві пристрої (монітори,

принтери та інш.), вводу з клавіатури, сканера тощо, в процесі її кодування-декодування та вироблення-перевірки підпису, що обумовлює необхідність використання екранованих приміщень. ЕОМ в захищеному виконанні, які відповідають вимогам ГОСТ 29339-92, дозволяють працювати з криптозасобами і в звичайних приміщеннях.

Вимоги ГОСТ 29339-92 до ЕОМ в захищеному виконанні не є недосяжними. Так, авторам довелось приймати участь в проведенні приймальних та кваліфікаційних випробувань ЕОМ загального призначення в захищеному виконанні "Плазма-ЗВ", що за рівнем захищеності не поступається кращим світовим зразкам та має значні запаси відносно вимог ГОСТ 29339-92.

При цьому слід підкреслити, що вартість ЕОМ «Плазма-ЗВ», призначеної для обробки ІзОД будь-якого ступеня секретності на одній і тій же ЕОМ на об'єктах будь-якої категорії, відповідає вартості згаданих раніше «ЕОМ II категорії».

Впровадження підходу щодо визначення "надзвичайних умов розташуваня" зазначених вище об'єктів державної влади та управлння, а також застосування в практичній діяльності вимог ГОСТ 29339-92:

- значно зменшить можливість перехоплення ІзОД, насамперед державної таємниці, порушення її цілісності та блокування, що підвищить рівень інформаційної безпеки як складової частини національної безпеки України;
- збереже бюджетні кошти за рахунок економії на спорудженні екранованих приміщень та обладнанні державних установ додатковими засобами захисту;
- дозволить, враховуючи міждержавний статус ГОСТ 29339-92, експортувати ЕОМ в захищеному виконанні українського виробництва, зокрема, до інших країн СНД;
- сприятиме зниженню рівнів електромагнітного випромінювання та його впливу на персонал, перш за все при значній насиченості засобами обчислювальної техніки робочих приміщень, особливо екранованих.

Література: 1. Сборник научных трудов "Защита информации" – Киев, КМУГА, 1999. 2. Материалы международной научно-технической конференции "Повышение эффективности систем защиты информации" "Защита-97" - Киев: КМУГА, 1997. 3. Фортов В.Е., Парфенов Ю.В., Лоборев В.М. "Электромагнитный терроризм: возможные последствия, методы и средства борьбы с новыми угрозами". 4. Торокин А.А. "Основы инженерно-технической защиты информации" – М.: Издательство "Ось-89", 1998. 5. Хорев А.А." Способы и средства защиты информации" – М., МО РФ, 1998. 6. Защита информации. Конфидент, № 1, 1998.

УДК 621.758.002

ЗАДАЧИ ЭЛЕКТРОМАГНИТНОЙ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ОСНОВНЫХ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СРЕДСТВ

Юрий Зиньковский, Вадим Клименко

Национальный технический университет Украины КПИ.

Аннотация: **Определены задачи экранирования компьютеров при возрастании их производительности и быстродействия. Информационная защита современных компьютеров - проблема сверхвысоких частот. Высокую эффективность экранирования обеспечивают многослойные экраны с чередующимися магнитными и немагнитными слоями. Металлизация пластмассовых корпусов осуществляется вакуумным напылением тонких (десятки микрометров) многослойных экранов. Разработанные численные методики расчета целевых показателей электромагнитной информационной защиты средствами экранирования в перспективе пригодны для расчета экранов в диапазоне от низких частот до СВЧ. Процесс разработки и внедрения в производство отечественных информационно - защищенных компьютеров должен быть непрерывным.**

Summary: **Determined tasks of shielding of computers. Information protektion of computers-problems of super high freguency, where multi-lager shields are effective. Proposed the technigue of callculation.**

Ключевые слова: **Защита информации банковских систем электронных платежей.**

I Постановка задачи

Обеспечение системных свойств электромагнитной совместимости и информационной защищенности для современных компьютеров не менее актуально, чем достижение совершенной функциональной полноты,