УДК 621.618

В.Д. Карлов[1], О.В. Лукашук[1], С.М. Шолохов[2]

[1] *Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків*
[2] *В/ч А1906*

ОСОБЛИВОСТІ ТЕХНІЧНИХ МЕТОДІВ ЗНИЖЕННЯ УРАЗЛИВОСТІ СИСТЕМ ТЕЛЕКОМУНІКАЦІЙ

У статті проведено аналіз забезпечення інформаційної безпеки у системах телекомунікацій. Проведений аналіз дозволив визначити коло питань, які методично повинні бути розглянуті для зниження уразливості систем при атаках на них, що носять електромагнітний характер, особливо при проведенні антитерористичної операції (АТО). Наведено основні типи завдань перехоплення інформації за рахунок побічних електромагнітних випромінювань.

Ключові слова: *інформаційна безпека, система телекомунікацій, захист інформації, електромагнітна хвиля, електромагнітна сумісність.*

Вступ

Постановка проблеми. Захист інформації в комп'ютерній техніці і обчислювальних мережах має більш, ніж 30-річну історію, тому до теперішнього часу вже накопичений значний досвід, як теоретичних розробок різних аспектів даної проблеми, так і практичного вирішення завдань захисту. Проте, на Україні питанню захисту інформації було приділено мало уваги і тому загальнодоступних публікацій [1, 2] з даної тематики практично не було. Останнім часом положення істотно змінилося, проте знадобиться якийсь час для того, щоб можна було скласти достатньо повну вибірку відповідних робіт.

В результаті аналізу практичного досвіду захисту від витоку інформації слід зазначити, що для телекомунікаційних систем спецпризначення (державних, військових, галузей промисловості) розробка механізмів захисту інформації була обов'язковою, і всі системи такі механізми мають. У всіх відомих системах основні зусилля були зосереджені на запобігання просочуванню інформації за рахунок перешкод і наведень. Для цих каналів розроблено як норми захищеності, так і необхідні для захисту засоби. Надмірна закритість всіх робіт по захисту інформації привела до того, що у відкритих телекомунікаційних системах по обробці даних, які складають основну масу функціонуючих систем, захист інформації практично відсутній зі всіма витікаючими звідси наслідками.

Окрім цього, телекомунікаційні системи у зв'язку з розвитком глобальних мереж отримали додатковий імпульс в своєму розвитку, технічна реалізація яких в межах будівель і приміщень отримала своє логічне завершення у вигляді загальнодоступних структурованих кабельних систем. Слід врахувати і підвищену насиченість навколишнього середовища різноманітними радіоелектронними засобами різного призначення, що приводить до електромагнітних обурень, які можуть порушити цілісність сигналу. Тому в даній статті розглянуто один з можливих підходів до рішення задачі захисту інформації технічними методами, які вельми близькі до прийомів забезпечення електромагнітної сумісності технічних засобів.

Виклад основного матеріалу

Можливі канали перехоплення інформації представлені на рис. 1.

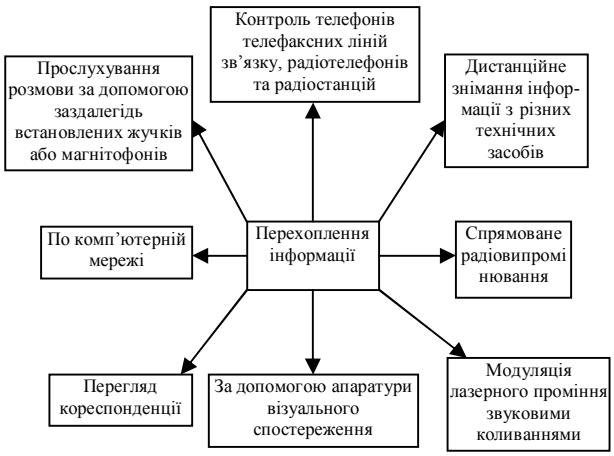

Рис. 1. Можливі способи перехоплення інформації

Виникає необхідність і право підприємства на захист своїх інтересів у взаєминах з іншими суб'єктами ринкових відносин. Привласнення машинної інформації, наприклад, шляхом перехоплення її за рахунок побічних електромагнітних випромінювань від комп'ютерної техніки, офісного устаткування, кабельної системи не кваліфікується як розкрадання, оскільки розкрадання зв'язане з вилученням цінностей з фондів організації. Машинна інформація є самостійним предметом кримінально-правової охорони.

Сучасний рівень розвитку радіотехніки, електроніки, обчислювальної техніки, методів аналізу,

криптографії дозволяє за сприятливих умов виділити сигнали, що несуть оброблювану телекомунікаційною системою (ТС) інформацію, із загального потоку електромагнітних випромінювань, що виникають при роботі пристроїв обчислювальної техніки, і відновити цю інформацію за допомогою спеціальних методів обробки прийнятих сигналів. Витік інформації за рахунок побічних електромагнітних випромінювань (ПЕМВ) є одні з основних каналів. Тому у всьому світі гостро стоїть проблема захисту оброблюваної в ТС інформації [1 – 4].

Для вирішення питання про необхідний ступінь захисту і оцінку захищеності інформації від витоку по каналах ПЕМВ необхідно спиратися на модель можливого перехоплення інформації. Для цього потрібно оцінити оперативно-тактичні, електродинамічні, технічні і алгоритмічні можливості перехоплення інформації.

При побудові моделі можливого перехоплення інформації слід враховувати той факт, що ефективне перехоплення інформації по каналах ПЕМВ є в переважній більшості випадків дуже складним завданням, як в технічному, так і в математичному плані. Тому удаватися до використання каналів ПЕМВ доцільно лише тоді, коли іншими, доступнішими методами добути інформацію не представляється можливим.

Для ефективного перехоплення сигналів в каналах ПЕМВ, взагалі кажучи, потрібна приймальна апаратура, здатна виділити конкретні сигнали від пристроїв ПЕОМ на тлі перешкод, що є адитивною сумішшю природних і штучних перешкод. Причому до останніх відносяться і перешкоди, що створюються самим даним технічним засобом ПЕОМ і сусідніми з ним компонентами ТС, а також структурованою кабельною системою. Такими можливостями володіють спеціалізовані кореляційні приймачі. У ряді випадків при перехопленні потрібно проводити накопичення фрагментів випромінювання з метою ефективного виділення корисних сигналів, що періодично повторюються, на тлі маскуючих перешкод (так званий прийом з накопиченням). Така апаратура також відноситься до спеціальної. Таким чином, приймальні пристрої, що серійно випускаються, в переважній більшості випадків не можуть бути ефективно використані для вирішення завдань перехоплення.

Проте є випадки, коли перехоплення виявляється можливим за допомогою серійної апаратури, що випускається.

Перший випадок – перехоплення висвічуваної на дисплеї інформації за допомогою звичайного телевізійного приймача. При цьому можна істотно поліпшити можливості прийому за допомогою незначних змін в телевізійному приймачі (рис. 2).

Другий випадок – перехоплення випромінювань від низькочастотних електромеханічних пристроїв з послідовним кодом передачі інформації. В цьому випадку перехоплення може бути здійснений достатньо вузькосмуговим приймачем, що серійно випускається.

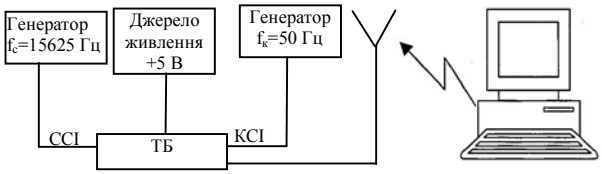

Рис. 2. Комплекс перехоплення електромагнітних випромінювань персонального комп'ютера

Оцінка алгоритмічних можливостей. Під алгоритмічними можливостями маються на увазі можливості відновлення оброблюваної ПЕОМ інформації за наслідками перехоплення сигналів в каналах ПЕМВ. Сюди відноситься розробка алгоритмів попередньої обробки суміші (корисний сигнал + перешкода), що приймається, з метою виділення сигналів, що несуть інформацію, на фоні перешкодових сигналів і шуму. Такі алгоритми закладаються в спеціалізовану апаратуру перехоплення при її проектуванні. Подальша обробка результатів прийому проводиться відповідно до спеціальних алгоритмів, що дозволяють відновити початкову інформацію. Така робота вимагає окрім знання техніку роботи з алгоритмами ще і великого досвіду по їх застосуванню і хорошого знання проблеми, до якої відноситься перехоплювана інформація.

Таким чином, навіть у разі застосування імпортної спеціалізованої апаратури перехоплення необхідно привертати фахівця в області відновлення інформації за наслідками прийому сигналів ПЕМВ, обізнаного проблему, до якої відноситься перехоплювана інформація.

У разі перехоплення інформації, що відображається на дисплеях, за допомогою телевізійних приймачів не потрібна ніякої додаткової обробки – вона просто прочитується з телевізійного приймача.

Граничні можливості по відновленню інформації за наслідками перехоплення за умови наявності необхідних апріорних даних, участі висококваліфікованих фахівців і використання могутніх обчислювальних систем свого часу оцінені, і результати відбиті у відповідних документах.

Оцінка оперативно-тактических можливостей. Досвід говорить, що можна практично безкарно і без перешкод відкрито займатися перехопленням випромінювань в безпосередній близькості до території підприємства. Тільки власна служба безпеки власника інформації може перешкодити (наскільки це виявиться можливим в рамках закону) займатися перехопленням ПЕМВ.

З погляду устаткування пункту перехоплення можна сказати наступне. Безумовно, не можна пов-

ністю виключити можливість придбання спеціалізованої апаратури.

Така вірогідність збільшується у разі організації окремих приватних підприємств, що спеціалізуються в області розкрадання інформації по замовленнях конкуруючих підприємств. В цьому випадку різко підвищується небезпека розкрадання інформації, оскільки такі утворення володітимуть ширшими фінансовими можливостями і можуть використовувати фахівців як в області радіоперехоплення, так і в області спеціальної математичної обробки результатів перехоплення з метою відновлення оброблюваної ПЕОМ інформації.

Електродинамічні обмеження перехоплення інформації. На об'єм і якість перехопленої інформації впливають електродинамічні процеси і обмеження, пов'язані з можливістю розповсюдження електромагнітних хвиль (ЕМХ) в заданій обстановці, певному середовищі. Для управління середовищем розповсюдження ЕМХ і локалізації електромагнітного поля повинне застосовуватися ефективне екранування, причому не тільки технічних компонентів телекомунікаційних систем, але і приміщень, в яких інсталюється ТС. Це говорить про комплексність проблеми забезпечення інформаційної безпеки, яка повинна вирішуватися на всіх етапах створення телекомунікаційної системи: від опрацьовування її концепції до інсталяції і виводу з процесу експлуатації.

Розширене розуміння питань інформаційної безпеки вимагає окрім розгляду ПЕМВ, говорити ще про цілісність сигналу.

Зловмисне спотворення інформаційного сигналу в телекомунікаційній системі може привести до втрати інформації або її спотворення. Ці спотворення, у свою чергу, відносно просто викликати інжекцією перешкод в мережу живлення телекомунікаційної системи, могутнім електростатичних розрядом, порушенням заземлення системи.

Подібні прийоми, потрапляючи до рук зловмисників, можуть привести до істотного збитку, і вже отримали в західній літературі назву "Електромагнітний тероризм".

Висновки

Таким чином, на сучасному етапі представляється розумним враховувати в моделі перехоплення два можливі варіанти залежно від ступеня важливості приховуваної інформації.

Для менш важливою, інформації можна вважати, що перехоплення ведеться виходячи з умов з обмеженими пізнаннями в області перехоплення ПЕМВ і не спеціалізованою апаратурою. Ці моделі припускають адекватні заходи захисту телекомунікаційної системи по перекриттю каналів просочування інформації за рахунок ПЕМВ.

Список літератури

1. Петраков А.В. Основы практической защиты информации / А.В. Петраков. – М: Радио и связь, 2000. – 368 с.

2. Ярочкин В.И. Информационная безопасность / В.И. Ярочкин. – М.: Междунар. отношения, 2000. – 400 с.

3. Руснак І.С. Розвиток форм і способів ведення інформаційної боротьби на сучасному етапі / І.С. Руснак, В.М. Телелим // Наука і оборона. – 2000. – № 2. – С. 18-23.

4. Петров В.Л. Применение нейрофизио-логической концепции интеллектуальной деятельности человека для моделирования сложных систем управления – объектов информационного противоборства / В.Л. Петров, С.Н. Шолохов, А.В. Снегуров // Зб. наук. пр. – Х.: ХВУ. – 2001. – № 4 (34). – С. 60-66.

Надійшла до редколегії 16.06.2016

Рецензент: д-р техн. наук, проф. Л.Ф. Купченко, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків.

ОСОБЕННОСТИ ТЕХНИЧЕСКИХ МЕТОДОВ СНИЖЕНИЯ УЯЗВИМОСТИ СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ

В.Д. Карлов, Е.В. Лукашук, С.Н. Шолохов

В статье проведен анализ обеспечения информационной безопасности в системах телекоммуникаций,. Проведенный анализ позволил определить круг вопросов, которые методически должны быть рассмотрены для снижения уязвимости систем при атаках на них, носящих электромагнитный характер, особенно при проведении антитеррористической операции (АТО). Приведены основные типы задач перехвата информации за счет побочных электромагнитных излучений.

Ключевые слова: *информационная безопасность, система телекоммуникаций, защита информации, электромагнитная волна, электромагнитная совместимость.*

FEATURES OF TECHNICAL METHODS OF VULNERABILITY DECLINE OF TELECOMMUNICATIONS SYSTEMS

V.D. Karlov, E.V. Lukashuk, S.M. Sholokhov

In the article the analysis of providing of informative safety is conducted in the systems of telecommunications,. The conducted analysis allowed to define the circle of questions which methodically must be considered for the decline of vulnerability of the systems at attacks on them, carrying electromagnetic character, especially during the leadthrough of anti-terror operation (ATO). The basic types of tasks of intercept of information are Resulted due to side electromagnetic radiations.

Keywords: *informative safety, system of telecommunications, priv, hertzian wave, electromagnetic compatibility.*