- контроль целостности, доступности и наблюдательности объектов защиты КС;
- експертная оценка информационной и антивирусной безопасности объектов защиты КС для оценки их соответствия заданным требованиям.

Наконец, выполнение предложенных рекомендаций носит не только теоретический характер (методологический, методический, концептуальный, отечественно приоритетный) , но и практический. Это обусловлено тем, что все существующие технологии защиты безопасности компьютерных систем и сетей не стопрцентны по надежности и это вполне закономерно, так как абсолютно надежной защиты КС не существует вообще, поскольку ситуация безопасности носит всегда дуэльный характер по общеизвестному принципу противоборства интересов: с одной стороны - пользователя КС и с другой стороны – нарушителей реализации или соблюдения их интересов.

Кроме того, дело в том, что любая защита не может быть универсальной вообще, она всегда конкретна под определенные угрозы, для конкретных объектов КС, под конкретную конфигурацию КС, под конкретно выбранную политику безопасности КС, при использовании конкретных функциональных (услуги К,Ц,Д,Н) и гарантийных (Г-1…Г-7) услуг безопасности, а также при конкретной степени их реализации по критерию «вид информационной деятельности с использованием КС-эффективность безопасности - гарантия безопасности - стоимость безопасности» и др.

Список литературы

1. *Шорошев В.В.* Недостатки традиционных средств защиты корпоративных сетей Интранет и необходимость применения новых методов их защиты. Бизнес и безопасность № 2, 2003, с.54-59;

2. *Шорошев В.В.* Перспективный метод защиты инормационных ресурсов корпоративных сетей Интранет. Бизнес и безопасность № 6, 2003, с38-46;

3. *В.Шорошев.* Перспективный метод защиты инормационных ресурсов корпоративных сетей Интранет. Науково-технічний збірник НТУ «КПІ» № 7, 2003. С.62-77;

4. *Rebecca Gurley Bace*. Intrusion Detection. Macmillan Technical Publishing, 2000;

5. *Panagiotis A* stithas. Intrsion Detection Systems. 1999;

6. [Cannadyl-98] James Cannady. Atificial Neural Networks for Misuse Detection. 1998;

7. *Грег Шипли.* Оружие компьютерного подполья. Сети и ситемы связи, № 10, 2000;

8. *Лукацкий А.В.* Обнаружение атак. – 2-е изд., перераб. и доп. - СПб.: БХВ-Петербург, 2003. – 608 с.: ил.

УДК 004.056.5

Васильцов І.В., Дубчак Л.О.

КЛАСИФІКАЦІЯ СУЧАСНИХ АТАК СПЕЦІАЛЬНОГО ВИДУ НА РЕАЛІЗАЦІЮ

Вступ

Задача захисту інформаційних ресурсів постає особливо гостро в умовах розвитку сучасних інформаційних технологій. Постійне зростання об'ємів інформаційних ресурсів обумовлює жорсткі вимоги до засобів шифрування/дешифрування стосовно швидкості опрацювання вхідних даних. Природно, що для вирішення цієї задачі необхідно використовувати апаратну реалізацію відомих алгоритмів криптографічного захисту інформації [1-3, 4-5].

Проте такі тенденції до апаратної реалізації засобів криптографічного захисту інформації в свою чергу обумовили появу принципово нових видів криптоаналізу, які умовно можна назвати "Атаки спеціальних впливів" або ж "Атаки на основі нестандартних

(побічних) каналів витоку інформації" (англ. мовою *side-channel attacks, covert-channel attacks*) [1,6,7]. Тому розробка підходів, методів, алгоритмів та засобів проектування криптографічних пристроїв захисту інформації, що є стійкими до такого виду атак є важливою та актуальною задачею.

На рисунку 1 зображено модель типового процесу передачі інформації по незахищених каналах зв'язку із врахуванням нестандартних каналів витоку інформації.

З рисунку видно, що окрім каналу, по якому передається шифротекст *C* (який традиційно утворюється шляхом криптографічного перетворення вихідного повідомлення *M* за умови використання ключа *k* і, який може бути доступним зловмиснику в умовах виконання пасивної атаки прослуховування), існує також інша додаткова інформація, що може бути використана криптоаналітиком для ефективної реалізації атаки на систему захисту інформації: звук, енергоспоживання, час виконання, електромагнітне випромінювання і т.п. У [6,7] показано, що така додаткова інформація дозволяє різко підвищити імовірність успішного виконання атаки за рахунок зменшення її складності.

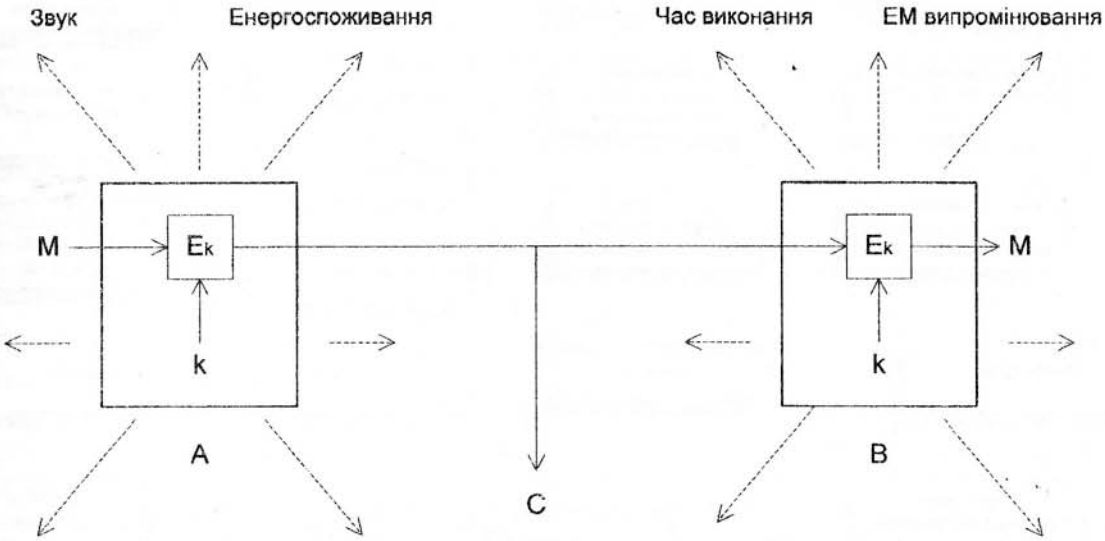

Рис 1. Модель типового процесу передачі інформації по незахищених каналах зв'язку

Канали витоку та перехвату інформації

Сучасні системи обробки таємної та конфіденційної інформації являють собою складні програмно-апаратні комплекси, що володіють специфічними каналами витоку інформації, що супроводжують штатний процес обробки інформаційних ресурсів. На рисунку 2 зображено класифікацію каналів витоку та перехвату інформації, отриману на основі аналізу [8-13].

Однією із основних вимог комплексного захисту є системний підхід, тому при виявленні технічних каналів витоку інформації необхідно розглядати усю сукупність елементів захисту, включаючи основне обладнання технічних засобів обробки інформації (ТЗОІ), кінцеві пристрої, з'єднувальні лінії, розподілюючі та комутаційні пристрої, системи електропостачання, заземлення і т.п.

Поряд із основними технічними засобами, що безпосередньо залучені до обробки та передачі інформаційних ресурсів, необхідно враховувати також допоміжні технічні засоби та системи (ДТЗіС) такі, як технічні засоби відкритого телефонного, факсимільного зв'язку, системи охоронної та пожежної сигналізації, електрифікації, радіофікації, електропобутові пристрої та інші струмопровідні металоконструкції.

Відповідно до способів перехвату інформації, від фізичної природи, а також середовища розповсюдження канали витоку та перехвату інформації можна розділити на

електромагнітні, електричні, акустичні, кабелі локальних обчислювальних мереж (ЛОМ), візуальні, індукційні, параметричні, закладки та віруси (див.рис.2).

Для електромагнітних каналів характерним є побічне випромінювання таких типів [8,10]:

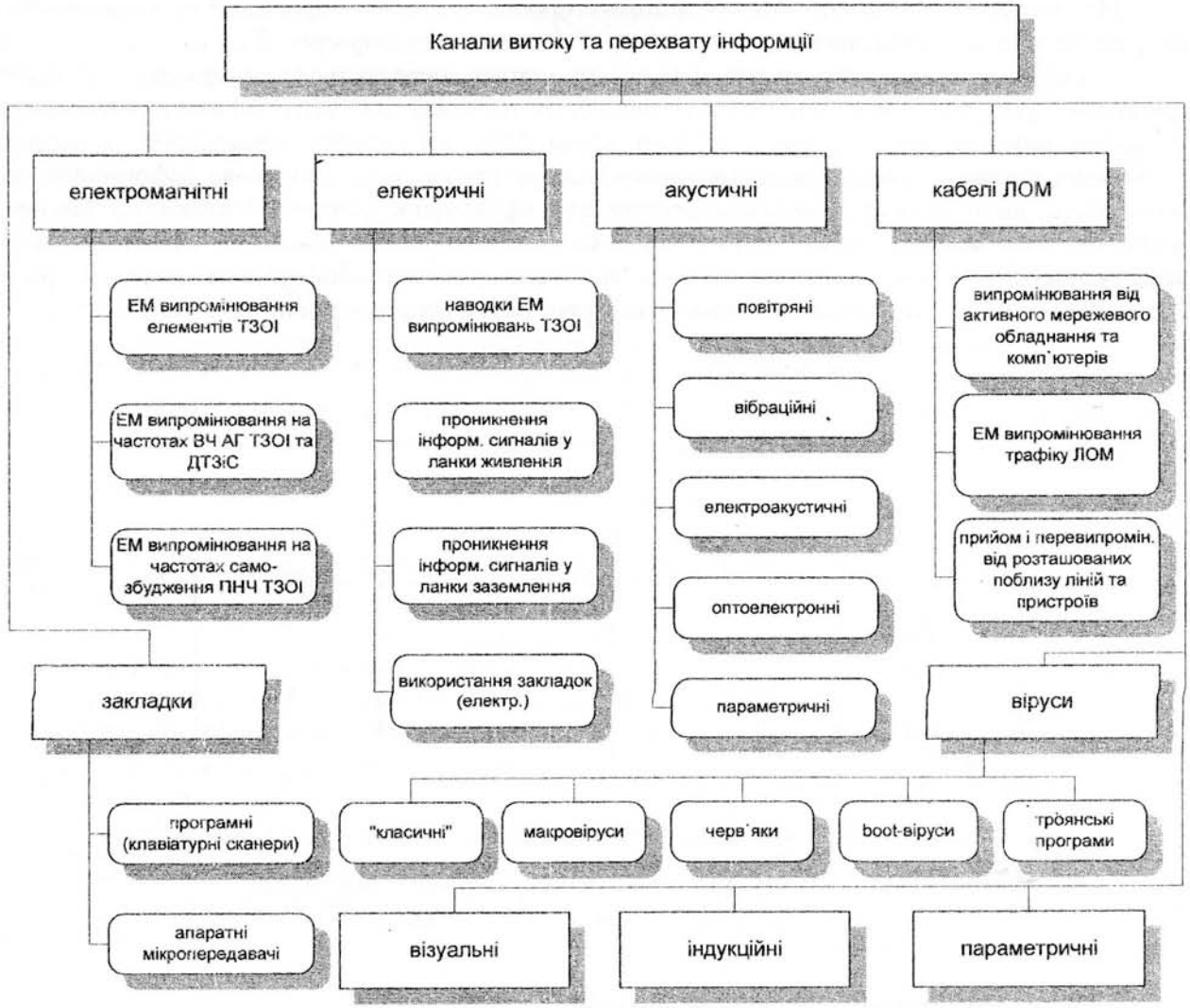

Рис 2. Класифікація каналів витоку та перехвату інформації

1) електромагнітне (ЕМ) випромінювання елементів ТЗОІ (носієм інформації є електричний струм, сила струму, напруга, частота або фаза якого змінюються за законом інформаційного сигналу);

2) ЕМ випромінювання на частотах роботи високочастотних генераторів ТЗОІ та ДТЗіС (внаслідок зовнішніх впливів інформаційного сигналу на елементах генераторів наводяться електричні сигнали, що можуть викликати незловмисну модуляцію власних високочастотних коливань, та випромінювання їх в оточуюче середовище);

3) ЕМ випромінювання на частотах самозбудження підсилювачів низької частоти ТЗОІ (самозбудження виникає внаслідок виникнення випадкових перетворень від'ємних зворотних зв'язків в паразитні додатні, що призводить до переведення підсилювача з режиму підсилення у режим автогенерування сигналу модульованого інформаційним сигналом).

Можливими причинами виникнення електричних каналів витоку є [8,10]:

1) наводки ЕМ випромінювань елементів ТЗОІ (виникають при випромінюванні ТЗОІ інформаційних сигналів, а також при наявності гальванічного зв'язку з'єднувальних ліній ТЗОІ та побічних провідників та ліній ДТЗіС);

2) проникнення інформаційних сигналів в мережі електропостачання (можуть виникати при наявності магнітного зв'язку між вихідним трансформатором підсилювача та трансформатором електропостачання, а також за рахунок нерівномірного навантаження на випростувальний пристрій, що приводить до зміни споживаного струму за законом зміни інформаційного сигналу);

3) проникнення інформаційних сигналів в ланки заземлення (можуть виникати при наявності гальванічного зв'язку із заземленням різноманітних провідників, що виходять за межі зони контролю, в тому числі нульового проводу мережі електропостачання, екранів, металевих труб систем опалення та водопостачання, металевої арматури і т.п.);

4) перехват інформації з використанням закладних пристроїв (являють собою міні передавачі, що встановлюються в ТЗОІ, випромінювання яких модулюються інформаційним сигналом і приймаються за межами зони контролю).

Середовищем акустичних каналів витоку та перехвату інформації можуть бути повітря, конструкції будівель, труби водопостачання та опалення, а також інші тверді тіла. Серед акустичних каналів виділяють [11-12]:

1) повітряні (носієм інформації є повітря і для їх перехвату використовують мініатюрні високочутливі та вузько напрямлені мікрофони, що з'єднанні з диктофонами чи спеціальними міні-передавачами);

2) вібраційні (носієм інформації є вібруючі конструкції будівель в межах зони контролю, а для перехоплення інформації використовують контактні, електронні та радіостетоскопи);

3) електроакустичні (утворюються за рахунок перетворення акустичних сигналів в електричні, наприклад в телефонних апаратах з електромеханічними дзвінками);

4) оптоелектронні (утворюються при опроміненні лазерним променем вібруючих в акустичному полі тонких відбиваючих поверхонь, наприклад віконне скло, дзеркала, картини і т.п.);

5) параметричні (утворюються в результаті дії акустичного поля на елементи високочастотних генераторів та зміні взаємно розміщення елементів схем, провідників, дроселів і т.п., що призводить до зміни параметрів сигналу).

Слід зауважити, що акустичні канали можуть бути джерелом витоку не лише мовної інформації, але й інформації з механічних замків, ключів, інформації з принтера чи клавіатури ЕОМ тощо.

Кабелі ЛОМ виділені в окрему групу, оскільки сучасні системи обробки інформації побудовані на базі локальних комп'ютерних мереж і, як правило, таке кабельне господарство являє собою розвинуту мережу провідників різного типу. Кабельна система не містить в собі активних чи нелінійних елементів, тому сама по собі вона не може бути джерелом "побічних" випромінювань, проте кабельна система пов'язує між собою всі елементи комп'ютерної мережі. По ній передаються мережеві дані, але також вона є і приймачем усіх паразитних наведень і середовищем для переносу "побочних" ЕМ випромінювань [9]. Розрізняють такі причини виникнення каналів витоку та перехоплення інформації:

1) випромінювання від активного мережевого обладнання та комп'ютерів (внаслідок неоднорідності кабельної системи та заземлення інформація від клавіатури чи монітора може випромінюватися мережевою системою);

2) ЕМ випромінювання трафіку ЛОМ (існує множина атак спрямованих на аналіз трафіку ЛОМ для визначення критичних ділянок навантаження системи, тому така інформація є важливою для зловмисника);

3) прийом і перевипромінювання від розташованих поблизу ліній та пристроїв (кабельна система може розглядатися як антена для перевипромінювання інших пристроїв, наприклад телефонних чи факсимільних апаратів, модемів та ін.).

Візуальні канали витоку інформації широко використовувалися в епоху доком'ютерного захисту інформації та продовжують застосовуватися і тепер. Для цього використовують спеціальні технічні засоби оптичного, теплового та іншого випромінювання.

Для документування результатів спостереження проводять фотографування чи зйомку об'єктів. Для дистанційного збору інформації використовують відео-закладки.

Індукційний канал перехоплення інформації не потребує контактного підключення до каналів зв'язку, тому він найчастіше використовується для маскування самого процесу зйому інформації. Сучасні індукційні здавачі можуть знімати інформацію з кабелів, захищених не лише ізоляцією, але також і подвійною стальною стрічкою з стальним дротом, що щільно обвивають кабель.

Параметричний канал витоку інформації формується шляхом високочастотного опромінення елементів ТЗОІ, при взаємодії магнітного поля котрого із елементами ТЗОІ виникає перевипромінення електромагнітного поля, промодулюваного інформаційним сигналом.

Закладка - це спеціальний засіб, призначений для збору та подальшої ретрансляції конфіденційної чи таємної інформації. В сучасних комп'ютерних засобах можуть використовуватися як програмні, так і апаратні закладки (наприклад, програмні клавіатурні шпигуни, апаратні мікро радіопередавачі та ін.). Зрозуміло, що складність виявлення таких закладних засобів безпосередньо впливає на захищеність комп'ютерних інформаційних ресурсів, що знаходяться в системі.

Сучасні комп'ютерні віруси володіють широким спектром можливостей зловмисного впливу. Дослідженню цієї проблеми присвячено широкий спектр публікацій. Загалом можна виділити такі категорії сучасних вірусів [13]:

1) традиційні (що базуються на використання спеціального коду для зараження інших файлів для переміщення між інформаційними ресурсами);

2) макровіруси (що базуються на використання макросів мови високого рівня для зараження та зловмисних дій);

3) троянські програми (маскуються під корисні програмні засоби, але володіють зловмисними функціями);

4) завантажувальні (що розміщуються в секторі завантаження операційної системи);

5) черв'яки (розповсюджуються лише мережею; тіло вірусу існує лише в процесі виконання вірусних операцій).

Хоча сучасні анти-вірусні засоби та технології інтенсивно розвиваються, проте вірусні канали витоку інформації можуть бути джерелом серйозних проблем конфіденційності інформаційних ресурсів.

Класифікація сучасних атак спеціального виду на пристрої захисту інформації

Хімічна комбінаторна атака - це спеціальний вид атаки на клавіатуру [14]. Атака полягає у нанесенні на кожну клавішу клавіатури невеликої кількості (кілька іонів) солі (наприклад, NaCl на клавішу "0", KCl на клавішу "1", LiCl на клавішу "2", SrCl2 на клавішу "3", BaCl2 на клавішу "4", CaCl2 на клавішу "5", і т.д.). В процесі натискання користувачем PIN-коду солі змішуються і це дає змогу використати таку інформацію для атаки. Оцінка зменшення ентропії завдяки хімічним слідам є досить цікавою комбінаторною задачею. За припущенням, що спектроскопічний аналіз мас дозволяє достатньо точно визначити компоненти суміші, в роботі [14] показано, що для наперед визначеного розміру PIN-коду атака дозволяє виявити введений персональний ідентифікаційний код користувача. Такий вид атаки може застосовуватися до клавіатури автоматичних дверей, телефонних апаратів, комп'ютерної клавіатури та навіть банкоматів. В роботі [14] наведено лише теоретичне обґрунтування ефективності такої атаки, проте експерти в сфері спектроскопічного аналізу мас підтверджують можливість успішної технічної (хімічної) реалізації такої атаки.

Звукова атака - класичний спосіб атаки на криптосистему з механічними та електричними замками, кодовими клавіатурами і т.п., які під час виконання різних операцій (наприклад, набір PIN-коду банкомата) випромінюють звуки. Якщо в клавіатурі банкомата чи номеронабирача телефону використовується тональна сигналізація натискання клавіш, то ця інформація може бути зчитана зловмисником і аналіз її дозволяє легко отримати

секретний PIN-код. У випадку, коли звукова сигналізація є моно-тональною, то атака дещо ускладнюється і перетворюється на комбінаторну задачу. Проте за умови використання нескладних алгоритмів аналізу та помірних обчислювальних ресурсів (оскільки більшість PIN-кодів банкоматів є чотиризначними) можна аналізувати паузи між звуковими сигналами для оцінки віддалі між натиснутими клавішами на клавіатурі, а відтак отримати імовірності натиснутих комбінацій.

Атака "чорний ящик" - це один із класичних методів зворотного інжинірингу (reverse engineering) мікросхем [15]. Суть атаки полягає в тому, що зловмисник подає на входи усі можливі комбінації сигналів та спостерігає реакції на виходах пристрою. На основі цієї інформації зловмисник може відтворити внутрішню логіку ПЛІС за допомогою карт Карно чи використовуючи спеціальні алгоритми спрощення вихідних таблиць. Такий вид атаки може бути застосований лише до ПЛІС невеликого розміру та за умови доступу до значних комп'ютерних ресурсів. Складність такої атаки суттєво зростає із збільшенням складності ПЛІС та використанням в логічній структурі пристрою цифрових автоматів, регістрів зсуву зі зворотними зв'язками (LFSR - Linear Feedback Shift Register), інтегрованих накопичувачів і т.п.

Зворотнє зчитування конфігурації ПЛІС

Зворотнє зчитування - це спеціальна функція, що притаманна більшості сучасних класів ПЛІС [15]. Ця функція дозволяє провести зчитування конфігурації ПЛІС для подальшого відлагодження. Суть атаки полягає в тому, щоб зчитати конфігурацію ПЛІС через відповідний інтерфейс (наприклад, JTAG чи програмний) та отримати таємну інформацію (наприклад, ключі). Функція зворотного зчитування може бути заблокована шляхом використання секретних бітів від виробника. Такий підхід запатентовано в США [16]. Проте існує імовірність, що зловмисник може обійти цей захист шляхом застосування атаки апаратних помилок для інвертування секретних бітів. Якщо це йому вдасться, то він отримає можливість зчитати конфігурацію ПЛІС і при потребі виконати клонування крипто-пристрою.

Перехоплення біт-потоку

У загальному випадку дані конфігурації зберігаються зовні у незахищеному вигляді і завантажуються в ПЛІС під час вмикання, щоб конфігурувати пристрій. Зловмисник може легко перехопити передачу біт-потоку та отримати файл конфігурації.

Фізичні атаки

Мета фізичної атаки полягає у дослідженні особливостей реалізації пристрою в мікросхемі, щоб отримати інформацію про алгоритми чи визначити секретні ключі шляхом дослідження області всередині кристалу ПЛІС. Таким чином, такі атаки орієнтовані на специфічні області ПЛІС, які є недоступними нормальним шляхом через входи/виходи. Це потенційно можна здійснити шляхом візуального спостереження, а також використовуючи спеціальні засоби такі, як оптичний, електронний мікроскоп чи механічні пробники. Проте, внаслідок збільшення складності ПЛІС, така атака може бути успішною лише за умови застосування складних методів з використанням систем сфокусованого променя іонів чи електронних мікроскопів [17].

Оптична атака апаратних помилок

Цей тип атак відноситься до фізичних напівруйнівних атак, метою яких є генерування збоїв у пристрої та подальше застосування диференційного криптоаналізу помилок [17]. Напівпровідникові транзистори, які є базою сучасних ПЛІС та мікро-контролерів, чутливіші до іонізуючого впливу, аніж вакуумні пристрої. Лазерне випромінювання може іонізувати область напівпровідника мікросхеми, якщо енергія фотону перевищує рівень енергії "ями" напівпровідника. Наприклад, лазерне випромінювання з довжиною хвилі 1.06 мікрометрів

(енергія фотона 1.17 електрон-Вольт) має глибину занурення 700 мікрометрів і забезпечує хороший рівень однорідності іонізації для напівпровідникових пристроїв.

Зчитування ЕМ випромінювання

Електромагнітні випромінювання виникають як результат зміни потоків струму в шинах керування, вводу-виводу, обробки даних та інших частин крипто-пристрою. Ці зміни струму та ЕМ випромінювання можуть бути як очікуванні, так і неочікувані. Кожен компонент пристрою, через який протікає струм, випромінює ЕМ хвилі не лише свої власні (що базуються на його власних фізичних та електричних параметрах), але й результат ЕМ впливу від інших компонент внаслідок дії паразитних зв'язків та геометрії самої схеми. Зловмисник, як правило, зацікавлений у виявленні та накопиченні ЕМ випромінювань, спричинених операціями обробки даних. В пристроях CMOS (КМОН), в ідеалі, струм протікає лише у випадку, коли відбувається зміна логічного стану елементів пристрою. Ця зміна контролюється синхроімпульсом дельта-видної форми. Інколи це спричинює появу інших неочікуваних, "некорисних" ЕМ випромінювань. Такі ЕМ випромінювання несуть інформацію про потік струму, а відтак про події, що відбуваються протягом кожного синхроімпульсу. Оскільки кожен компонент крипто-пристрою виділяє різні типи ЕМ випромінювань, вони дозволяють отримати різні "описи" подій, що відбуваються протягом кожного синхроімпульсу. В цьому полягає відмінність від атаки аналізу енергоспоживання, в котрій в кожен момент часу доступний лише один "опис" зміни потоку струму і пояснює чому даний вид атаки є ефективнішим. Детальніший опис атаки такого виду можна знайти у [18].

Атака апаратних помилок

Суть атаки на основі апаратних помилок полягає у наступному: порушник має доступ до апаратури захисту інформації і має змогу проводити штатні операції стосовно криптографічного перетворення вхідних даних, а також може спеціальним чином впливати на процес обробки інформації, щоб спричинити некоректну роботу засобів захисту інформації, а відтак отримати спотворений шифротекст. Подальша робота полягає в аналізі (традиційно диференційному) криптотексту, отриманого у нормальному режимі роботи та у режимі виникнення помилок. Незважаючи на очікувану велику складність такого процесу, Е.Біхам та А.Шамір теоретично довели, що в загальному випадку достатньо від 50 до 200 пар незалежних криптотекстів для зламу алгоритму DES [19]. Тому зрозуміло чому інтенсивність наукових досліджень, присвячених захисту від атак спеціального виду, зростає. Актуальність проведення наукових досліджень в цій галузі обумовлюється ще й тим, що класично у якості криптопристрою розглядається електронна банківська картка, яка містить в собі ключі, котрими шифруються усі трансакції. Очевидно, що компрометація такого ключа може призвести до серйозних економічних втрат.

Одним із вузьких місць реалізації атаки на основі апаратних помилок є реалізація апаратних помилок. Розглянемо моделі реалізації апаратних помилок. Їх можна класифікувати таким чином:

1) реалізація спеціальних способів керування процесом криптографічної обробки інформації (вбудова додаткових сигнальних ліній, використання спеціальних кодових комбінацій, потаємних ходів і т.п. -- тобто неадекватне (недобросовісне) виконання проектування пристрою із зловмисним виконанням потаємних ходів та закладок);

2) реалізація постійних відмов (перепалювання комірок пам'яті, ліній зв'язку, створення відмов типу коротке замикання чи обрив і т.п.);

3) реалізація збоїв апаратури (використання зовнішніх впливів типу зміни температури навколишнього середовища, нестабільності напруги живлення, зміна тактової частоти роботи пристрою, електромагнітне випромінювання і т.п.).

Перевага застосування першої моделі полягає у можливості ідеальної синхронізації процесу перетворення інформації із реалізацією помилок, що є дуже важливим для

ефективної реалізації атаки. Проте такий підхід має суттєвий недолік - необхідно володіти доступом до процесу проектування, а також використовувати надлишковість в апаратній реалізації ліній зв'язку чи інформаційну надлишковість кодів керування і т.д., що може бути виявлено при детальнішому аналізі реалізації апаратних засобів.

Застосування другої моделі може використовуватися лише для зворотного трасування (атака лише на ключі (повідомлення), що вже були зашифровані), оскільки передбачає необхідність реалізації постійних відмов елементів (вузлів) апаратури. Окрім того, система захисту одразу ж виявить таку атаку на основі аналізу тестів функціонування апаратури.

У випадку успішної реалізації збоїв, зловмисник має змогу застосовувати атаки як "прямого", так і "зворотного" трасування. Це основна перевага застосування такої моделі, хоча для реалізації збоїв зловмисник повинен володіти певними засобами та досвідом.

Атака на час виконання окремих операцій

Час виконання криптографічних операцій залежить не лише від ефективності реалізації конкретного алгоритму, але й також (інколи суттєво) від вхідних даних [6, 20]. Особливо така кореляція сильно проявляється для алгоритмів модулярного експоненціювання асиметричних криптосистем та алгоритмів додавання (множення) точок на еліптичній кривій. Як правило, ці вказані криптографічні операції є обчислювально складними і для підвищення продуктивності виконання процедури шифрування повідомлення чи формування цифрового підпису використовують спеціальні алгоритми, які базуються на оцінці бітової інформації ключа шифрування. Така оцінка в алгоритмах дозволяє пришвидшити виконання криптографічних операцій за рахунок обходу виконання деяких операцій алгоритму при нульових бітах ключа. Звідси очевидно, що завжди можна виявити певну кореляцію між кількістю одиничних бітів ключа та часом виконання такого алгоритму. Саме така інформація дозволяє зловмиснику висунути гіпотезу щодо кількості одиничних та нульових бітів у секретному ключі, кількісним еквівалентом якої може бути вага Хемінга, а вже на основі такої оцінки здійснити атаку повного перебору вже в певному під-діапазоні ключового простору, що потребує значно менших обчислювальних ресурсів. Таким чином, оцінка кореляції часу виконання криптографічних операцій та ваги Хемінга ключової інформації дозволяє зловмиснику зменшити складність атаки на систему захисту інформаційних ресурсів.

Атака енергоспоживання

Електронні пристрої споживають струм з джерела струму протягом виконання операцій. Струм споживання змінюється в залежності від типів операцій, які ці пристрої виконують. Джерела струму більшості пристроїв надають константне значення енергії, тому зрозуміло, що енергія, яку споживає пристрій в процесі роботи є пропорційною до споживаного струму. Тому для проведення даної атаки зловмисник може використовувати як вимірювання споживаного струму, так і споживаної потужності. Більшість сучасних криптографічних пристроїв імплементуються в КМОН-технології. Дана технологія характеризується асиметрією стосовно напруги логічного значення нуля та одиниці. Основним логічним елементом в цій технології є інвертор, який побудований на двох транзисторах, що працюють як перемикачі, керовані напругою. В залежності від вхідного сигналу один із транзисторів відкривається (тоді як інший закривається) і на вихід інвертора подається або напруга живлення, або ж вихід закорочується на шину заземлення. Протягом перемикання з високого логічного стану у низький існує певний момент часу, коли обидва транзистори є відкритими. В цей момент струм з шини живлення стікає на шину заземлення внаслідок ефекту короткочасного короткого замикання між двома шинами. Це у свою чергу спричинює короткочасні паразитні імпульси в колі живлення та заземлення. Для здійснення атаки зловмисник може використовувати або аналіз особливостей асиметрії, або ж аналіз імпульсів, що виникають в колі джерела живлення [6, 21-22].

У пристроях з мікропроцесорами (таких як смарт-картки) протягом обчислення використовуються послідовності базових операцій (наприклад, LOAD, STORE), що спричиняють регулярні перемикання транзисторів. Відображення цих перемикань можна помітити на осцилограмах напруги джерела живлення як імпульси певної форми, що повторюються протягом роботи пристрою. В алгоритмах, що використовують ітеративну архітектуру обчислень, аналіз появи таких послідовностей дозволяє зловмиснику висувати гіпотези щодо підмножини ключів, що використовуються для крипто-перетворення.

На рисунку 3 зображено узагальнену класифікацію атак спеціального виду на криптопристрої. У якості ключових ознак наведено такі:

- за типом аналізованої інформації – дана ознака є найпопулярнішою і широко використовується для визначення який саме тип інформації з побічних каналів витоку лежить в основі криптоаналізу. Розрізняють такі види: атака апаратних помилок, аналіз енергоспоживання, аналіз електромагнітного випромінювання, часовий аналіз, хімічна комбінаторна атака;
- за методом виконання атаки – у свою чергу атака апаратних помилок в залежності від методики проведення спеціальних впливів на апаратуру може містити відмінні ключові операції самого криптоаналізу, тому розрізняють такі види: обнулення бітів ключа, інвертування бітів ключа, зчитування інформації з пам'яті;
- за кількістю аналізованих даних розрізняють звичайний та диференційний аналіз. Для звичайного аналізу достатньо лише одного (або кількох) сигналу, а диференційний аналіз використовують, щоб за допомогою статистичних методів усереднити та усунути випадкові та зумисні завади та виділити корисний сигнал з каналів витоку;
- за типом аналізованих даних диференційний аналіз ділиться на такі: за вагою Хемінга, SEMD – Simple Exponent Multiply Data (одна експонента, багато даних), MESD – Multiply Exponent Simple Data (багато експонент, одне дане), ZEMD – Zero Exponent Multiply Data (жодної експоненти, багато даних);
- за об'єктом аналізу розрізняють атаки на область команд та на область даних. Атаки на область команд мають за мету змінити порядок виконання операцій алгоритму;
- за рівнем деталізації атаки охоплюють усю ієрархію сучасних систем захисту інформації на рівні операцій, процедур, алгоритмів та цілої системи захисту;
- за об'єктом атаки поділяють на атаки на ключ та на алгоритм. У деяких випадках зловмиснику корисно атакувати не ключ, а сам алгоритм, наприклад, зменшити до мінімуму (однієї) кількість ітерацій і застосувати алгоритми квазі-повного перебору;
- за типом атаки бувають пасивні, коли зловмисник лише накопичує та аналізує дані, отримані по каналах витоку (наприклад, при часовому аналізі), та активні, у випадку коли зловмисник спеціальним чином діє на криптографічний пристрій, щоб спричинити появу каналів витоку, які за нормальних умов експлуатації не проявляються (наприклад, атака апаратних помилок);
- за природою аналізованих даних розрізняють прямі, у випадку коли отримані сигнали безпосередньо стосуються аналізованих криптографічних операцій (наприклад, при аналізі енергоспоживання), а також коли використовуються непрямі, модульовані, відбиті сигнали (наприклад, при аналізі електромагнітного випромінювання) .

Окремою категорією виділено атаки на ПЛІС – тут розглянуті типи атак, що стосуються лише систем захисту інформації, побудованих на ПЛІС і використовують саме специфіку проектування, виготовлення та експлуатації систем захисту інформації, у котрих ключові функції реалізовані на ПЛІС.

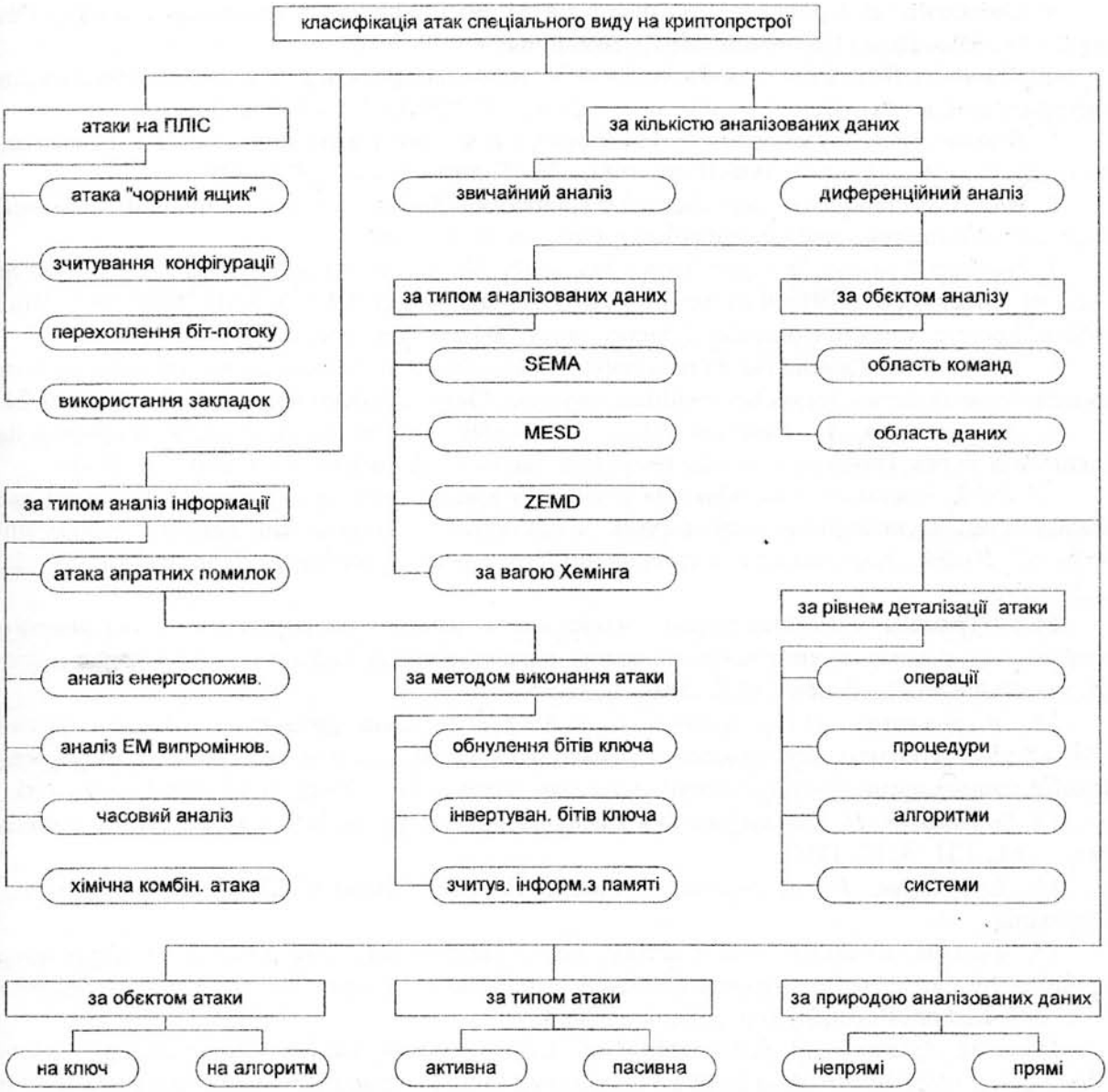

Рис 3. Узагальнена класифікація атак спеціального виду на криптопристрої

Висновки

У даній статті проведено класифікацію каналів витоку та перехвату інформації, отриману на основі аналізу сучасних досліджень у даній галузі. Подано аналіз можливих причин виникнення електромагнітних, електричних, акустичних, візуальних, індукційних та параметричних каналів витоку таємної інформації, а також розкрито суть виникнення витоку в кабелі ЛОМ. Розкрито також такі засоби збору таємної інформації як закладки та віруси.

Автори провели класифікацію сучасних атак спеціального виду на пристрої захисту інформації.

Аналіз описаних у статті каналів витоку таємної інформації та можливих атак на криптосистеми дозволяє побудувати стійкі системи захисту інформації.

Список літератури

1. *Чмора А.Л.*. Современная прикладная криптография.–2-е изд.– М.:Гелиос АРВ, 2002. – 256 с.

2. *Молдовян А.А., Молдовян В.А., Советов Б.Я.* Криптография. –Спб.: Издательство "Лань", 2000. – 224 с.

3. *Столлингс В.* Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Изд. Дом «Вильямс», 2001 – 672 с.: ил.

4. *Широчин В.П., Мухин В.В., Кулик А.В.* Вопросы проектирования механизмов защиты информации в компьютерных системах и сетях, - К., "ВЕК+", 2000. – 112 с., ил.

5. *Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях / Под ред. В.Ф.Шаньгина, - М.: Радио и связь, 1999. -328 с.

6. *Muir J.* Techniques of side channel cryptanalysis: Technical report / University of Waterloo. Dept. of Combinatorics and Optimization.– Waterloo (CA), 2001.

7. *François Koeune, François-Xavier* Standaert, 34. A Tutorial on Physical Security and Side-Channel Attacks, Foundations of Security Analysis and Design III : FOSAD 2004/2005, Volume 3655 of Lecture Notes in Computer Science, pages 78-108, November 2006.

8. *Зайчук А.В.* Основные пути утечки информации и несанкионированного доступа в корпоративных сетях. Науково-технічний журнал "Захист інформації" № 4, 2003, ст.19-24.

9. *Чеховский С.А., Рудаков Ю.М.* Побочные излучения и защита информации в локальных сетях. Науково-технічний журнал "Захист інформації" № 4, 2003, ст. 30-38.

10. *В.І.Заболотний.* Класифікація технічних каналів витоку інформації. Всеукраїнський міжвідомчий науково-технічний збірник "Радіотехніка". Тематичний випуск "Інформаційна безпека" №134, Харківський національний університет радіоелектроніки, Харків- 2003, ст.210-218.

11. *Журавель Т.Н.* Некоторые особенности защиты информации с ограниченным доступом от утечки по виброакустическому каналу. Защита информации: Сборник научных трудов. Выпуск 10. – Киев: НАУ, 2003, ст.91-95.

12. *Васильченко И.И., Кравченко И.А.* Магнитоэлектрические виброизлучатели с пониженным уровнем акустического шума для систем технической защиты информации. Защита информации: Сборник научных трудов. Выпуск 10. – Киев: НАУ, 2003, ст.96-105.

13. *Безруков К. Н.* Классификация компьютерных вирусов MS DOS и методы защиты от них. — М.; СП "ICE", 1990.

14. *Eric Brier, David Naccache, Pascal Paillier.* Chemical Combinatorial Attacks on Keyboards

15. *Thomas Wollinger and Christof Paar.* How Secure Are FPGAs in Cryptographic Applications? In 13th International Conference on Field Programmable Logic and Applications - FPL 2003, Lisbon, Portugal, September 1-3, 2003.

16. *J. M. Aplan, D. D. Eaton, and A. K. Chan.* Security Antifuse that Prevents Readout of some but not other Information from a Programmed Field Programmable Gate Array. United States Patent, No. 5898776, April 27 1999.

17. *Skorobogatov S., Anderson R.* Optical Fault Induction Attacks // Proc.of the 4th International Workshop CHES'2002.– San Francisco (USA), 2002.– P.2-12.

18. *Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi.* The EM Side-Channel(s). In Proceedings of 4th International Workshop on Cryptographic Hardware and Embedded Systems – CHES 2002, Redwood Shores, CA, USA, August 13-15, 2002, LNCS 2523, pp. 29 - 45.

19. *Biham E., Shamir A.* Differential Fault Analysis of Secret Key Cryptosystems // Proc. of the 17th Annual International Cryptology Conf. on Advances in Cryptology.– Santa Barbara (USA), 1997.– P.513-525.

20. *Васильцов І.В., Васильків Л.О.* Стійкість сучасних алгоритмів модулярного експоненціювання до часового аналізу - Науково-технічний журнал "Захист інформації", №1, 2005, С. 54-69

21. *Paul Kocher, Joshua Jaffe, and Benjamin Jun.* Differential Power Analysis // in Advances in Cryptology - CRYPTO'99 Proceedings of 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 1999. LNCS 1666, pp. 388-397

22. *Thomas S. Messerges, Ezzy A. Dabbish, and Robert H. Sloan*. Power Analysis Attacks of Modular Exponentiation in Smartcards // Cryptographic Hardware and Embedded Systems First International Workshop, CHES'99, Worcester, MA, USA, August 1999, LNCS 1717, pp. 144-157.

УДК 534.87:621.397.7:65.012.8(045) **Кучеренко М.А., Ткаліч О.П.**

КЛАСИФІКАЦІЯ ВИТОКІВ ІНФОРМАЦІЇ

По цій темі написано сотні робіт, проведено десятки конференцій, але багато з них не зрозумілі звичайному читачу. В цій статті розглядається найбільш доступна інформація, яка не потребує від читача поглиблених знань техніки. Аналізуються найбільш прості способи витоку інформації і рекомендації щодо запобігання її втрати.

З найдавніших часів будь-яка діяльність людей ґрунтувалася на отриманні й володінні інформацією, тобто на інформаційному забезпеченні. Саме інформація є одним з найважливіших засобів рішення проблем і завдань, як на державному рівні, так і на рівні комерційних організацій і окремих осіб. Одержання інформації шляхом проведення власних досліджень і створення власних технологій є досить дорогим, тому вигідніше витратити певну суму на придбання вже існуючих відомостей. Таким чином, інформацію можна розглядати як товар. А бурхливий розвиток техніки, технології та інформатики в останні десятиліття викликало ще більш бурхливий розвиток технічних пристроїв і систем розвідки. У створення пристроїв і систем ведення розвідки завжди вкладалися й вкладаються величезні кошти у всіх розвинених країнах. Сотні фірм активно працюють у цій області. Серійно виробляються десятки тисяч моделей «шпигунської» техніки. Тому останнім часом органи влади приділяють питанням захисту інформації більш пильну увагу. Ця галузь бізнесу давно й стійко зайняла своє місце в загальній системі економіки Заходу та має під собою міцну законодавчу базу у відношенні як юридичних, так і фізичних осіб, тобто суворо регламентована й реалізована в чітко налагодженому механізмі виконання. Тематики розробок на ринку промислового шпигунства охоплюють практично всі сторони життя суспільства, безумовно, орієнтуючись на найбільш фінансово-вигідні. Спектр пропонованих послуг широкий: від примітивних радіопередавачів до сучасних апаратно - промислових комплексів ведення розвідки. Звичайно, у нас ще немає великих фірм, які виробляють техніку подібного роду, немає й такої розмаїтності її моделей, як на Заході, але техніка вітчизняних виробників цілком може конкурувати з аналогічно західною, а іноді вона краще й дешевше. Природно, мова йде про порівняння техніки, що є у відкритому продажу. Апаратура ж, використовувана спецслужбами (її кращі зразки), набагато вища за рівнем своїх можливостей, за техніку, використовувану комерційними організаціями. Все це пов'язане з достатнім ризиком цінності різного роду інформації, розголошення якої може привести до серйозних втрат у різних галузях (адміністративної, науково-технічної, комерційної і т.п.). Тому питання захисту інформації (ЗІ) набувають все більш важливого значення.

Метою несанкціонованого збору інформації в цей час є, насамперед - комерційний інтерес. Як правило, інформація різнохарактерна, різноманітна й ступінь її таємності (конфіденційності) залежить від імені або групи осіб, кому вона належить, а також сфери їх діяльності. Діловій людині, наприклад, необхідні дані про конкурентів: їх слабкі й сильні сторони, ринки збуту, умови фінансової діяльності, технологічні таємниці. В політиці або у військовій справі виграш іноді виявляється просто безцінним, тому що політик, адміністратор або просто відома людина є інформантом. Цікаве його повсякденне життя, зв'язок в певних колах, джерела особистих доходів і т.п. А розвиток ділових відносин