4 Забезпечення захисту інформації в системах зв'язку. Технічні засоби системи захисту інформації

УДК 681.3

ФІЗИЧНА БЕЗПЕКА КОМП'ЮТЕРНОЇ СИСТЕМИ ТА ЇЇ ЗАБЕЗПЕЧЕННЯ ШЛЯХОМ ВИКОРИСТАННЯ РАДІОАКТИВНИХ МІТОК

Іван Пающик
НДІ НАВСУ

Анотація: **Розглядається один із аспектів фізичної безпеки комп'ютерної системи та її забезпечення шляхом реалізації програмно-апаратних засобів з використанням слаборадіоактивних кодованих міток.**
Summary: **In the article one is considered from aspects of physical safety of the computer system and it maintenance by realization program-hardware with use poorly radioactive of coded scores.**
Ключові слова: **Радіоактивна мітка, радіоізотоп, фізична безпека, маркер, маркування, кодований спосіб захисту, екстракоди, спецпроцесор.**

I Вступ

Згідно з вимогами НД ТЗІ 2.5-004-99 пункт 10.2 "Середовище розробки для забезпечення безпеки комп'ютерних систем" повинна використовуватися система заходів технічної, фізичної, організаційної і кадрової безпеки, спрямованої на захист усіх засобів і матеріалів, що використовуються для реалізації комплексу засобів захисту (КЗЗ) від несанкціонованої модифікації або руйнування [3, 4]. У підрозділі п. 10.2 "Керування конфігурацією" регламентована та визначена послуга фізичної безпеки комп'ютерних систем (КС) для рівнів гарантії безпеки Г-6, Г-7. Це нові вимоги до безпеки КС, у тому числі, щодо їх безпеки стосовно фізичного середовища. Безсумнівно, що це потребує подальшої розробки, у тому числі, фізичної безпеки комп'ютерної системи шляхом використання радіоактивних міток, що є темою статті.

II Постановка завдання

Основним завданням статті є висвітлення розроблених універсальних, латентних, машинозчитуємих способів і засобів захисту та їх реалізація для забезпечення фізичної безпеки складових і матеріалів, що використовуються для реалізації КЗЗ від загроз його несанкціонованої модифікації або руйнування. Досягається це шляхом використання новітніх технологій захисту з використанням слаборадіоактивних ізотопів.

III Основна частина

Для забезпечення фізичної безпеки комп'ютерних систем (їх елементів, вузлів, пристроїв, приладів, матеріалів, носіїв інформації тощо) пропонується їх маркувати радіоізотопами слабкої активності і використовувати ці маркування для автоматизованого машинозчитуємого контролю. Розроблено нові (отримано патенти на винаходи) латентні машинозчитувані радіоізотопні способи захисту – крапково-кодований, символьно-графічний щільно-кодований, багаторівневий кодований та комбінований, – які використовуються в залежності від рівня захисту, об'єкта захисту , поставленого завдання.

Переваги розроблених способів:

- препарат мітки або маркеру та радіоактивні ізотопи вузької дії їх використання знаходяться під державним контролем;
- строк дії мітки визначається відповідним радіоактивним ізотопом і знаходиться в межах від часів до тисяч років;
- можливість маркування любих твердих тіл;
- можливість кодування маркування;
- для збільшення рівня захисту препарат мітки кодується внутрішнім кодом – кількістю ізотопів та їх співвідношеннями;

- зчитування мітки не висуває умов до освітленості, температури тощо;
- нанесені мітки не змінюють властивостей предмету, що маркується;
- мітку не можуть знайти прилади, що випускаються серійно;
- координати мітки, тип, активність ізотопу можуть бути ідентифікаційними параметрами;
- мітки наносяться і перевіряються в автоматичному і ручному режимах.

Обмеження у використанні способів стосуються тільки рідин та газів. Розроблені способи відносяться до універсальних машинозчитуємих (машинопов‘язаних) способів захисту носіїв інформації, документів, предметів.

Сутність способів маркування предметів полягає у нанесенні препарату носія слаборадіоактивної кодованої мітки на їхню поверхню одним із методів: фізичним; хімічним, крапко-гальванічним, електроіскровим, іонно-плазмовим, а також шляхом введення слабко-радіоактивного нукліду у склад фарби (апробовано на фарбах та обладнанні інституту спецвидів друку з позитивним результатом, люмінесцентних пастах, чорнилах, інфрачервоних абсорберах, металевих наповнювачах, тощо).

Ідентифікація–зчитування кодованих міток відбувається спеціально розробленими засобами та приладами трьох рівнів.

Загальні характеристики способів і засобів захисту та деякі шляхи їх реалізації

Крапко-кодований слаборадіоактивний спосіб захисту (патент на винахід [1]). Спосіб дозволяє встановлювати на носій інформації та предмет спеціальним шляхом кодовану слаборадіоактивними індикаторами мітку (крапку), а також, при необхідності, геометричний реперний код та зчитування цієї мітки спеціальним приладом з відповідним геометричним реперним зчитувачем.

Спосіб та засіб можливо використовувати для локальної та загальної охорони носіїв інформації, предметів, у тому числі, предметів культурно-історичної спадщини держави (в межах приміщень, виставкових залів, окремих експонатів) та різних важливих компонентів систем обробки інформації та її технічного захисту (ТЗІ).

Слаборадіоактивна мітка має визначену (не точно дозовану) активність (мін. – мах.). На неї налаштований вузол зчитування та контролю, що входить до складу автономного приладу, виготовленого на базі недорогого надійного автономного процесору типу PIC, робота якого програмується для забезпечення охорони маркованого предмету згідно з правилами охорони або санкціонованого доступу, розробленими для відомства, організації, експозиції, приміщення.

Кількість нанесених кодованих розрядів на одиницю поверхні залежить від геометричних розмірів детекторів реєстрації випромінювання і для одного мільйона ознак дорівнює 26 кв. см. Носій інформації – предмет містить у собі нанесені слаборадіоактивні ізотопи.

Символьно-графічний щільно-кодований спосіб захисту та **пристрій** його реалізації (патент на винахід [2]). Спосіб прихованого символьно-графічного щільно-кодованого радіоізотопного захисту носіїв інформації, предметів за допомогою радіоактивних ізотопів-індикаторів полягає:

- в нанесенні слаборадіоактивного символьно-графічного **зображення** (та) або щільних **крапкових кодів** на носій інформації чи предмет;
- в ідентифікації їх пристроєм зміненої конструкції (міні телекамери) – матриці напівпровідникових приладів із зарядовим зв'язком (НПМЗЗ);
- кожен елемент такої матриці виконує функцію позиційного мікронапівпровідникового детектора реєстрації випромінювання, яке візуально відбивається на екрані монітору у вигляді короткої риски (пташки) при зчитуванні альфа, бета або гама частки;
- у подальшій комп'ютерній обробці зображень зчитуванням рисок (символів) по кожному рядочку кадру (режим рахування детекторів) та візуалізації символьно-графічного і (або) щільно-кодованого крапкового слаборадіоактивного зображення, яке знаходиться під матрицею НПМЗЗ з її довільною властивістю відбиття, шляхом накладення кадрів один на одного за розрахунковий проміжок часу;
- за необхідності, в обробці зображення методами математичної статистики.

Нанесена попереднім способом слаборадіоактивна крапка виглядає як неповторне, складне, з характерними зонами розподілу активності, кодоване, тримірне кольорове зображення. Спосіб дозволяє використовувати альфа, бета, гама ізотопи, а також їх комбінації з низькими енергіями та активністю. Носій інформації – предмет містить у собі нанесені радіоактивні ізотопи.

Багаторівневий прихований кодований спосіб захисту (розглядається держпатентом України). Винахід відноситься до способів багаторівневого прихованого кодованого способу захисту носіїв інформації, предметів шляхом їх кодування вкрапленням різнопитомих домішок і їх сумішей (алюмінію, талію, ванадію, бронзи, латуні, міді, сталі, пухирця повітря, і т. і.) з різними фізичними (товщина, пористість, щільність) і ядерними властивостями (заряди ядер відрізняються на чотири одиниці і більше), що наносяться у відповідному геометричному місці.

Ідентифікація вказаних **вкраплень** здійснюється методом абсорбції або зворотного розсіювання дії одного з колімованих корпускулярних мікро випромінювачів β-часток.

Це дає змогу забезпечити високий багаторівневий **кодований захист** паперових, пластикових та металевих носіїв інформації а також предметів із фарфору, скла, тканини, гуми, дерева завдяки багатомірному ідентифікаційному параметру (питома вага, товщина, пористість та щільність вкраплень, відсоткові показники двокомпонентних сплавів і сумішей, заряду атомного ядра, джерела корпускулярного випромінювання та їх комбінацій), що використовуються в одному із кодованих розрядів.

Носії інформації і предмет не містить в собі радіоізотопів. Вкраплення не активуються при ідентифікації під дією β-випромінювачів. Спосіб можливо використовувати для локальної (або загальної) експертної оцінки матеріалів разом із дрібними комплектуючими комп'ютерних систем (електронних плат та їх особливостей щодо мікроелементної бази, монтажу, порушення фізичної цілісності від еталонного зразка тощо).

Комбінований спосіб захисту носіїв інформації, предметів з використанням радіоактивних ізотопів (розглядається в Держпатенті України).

Цей спосіб базується на об'єднанні приладу реалізації символьно-графічного, щільно-кодованого, багаторівневого, прихованого, кодованого захисту шляхом використання **вкраплень** різних геометричних форм – трикутник, прямокутник, багатокутник, коло, тороїд тощо, – розмірами менших за 0.3 мм.

Для виконання поставленого завдання використовується розроблений в НДІ НАВСУ МВС та запатентований Держпатентом України крапково-кодований, слаборадіоактивний спосіб захисту предметів, цінних паперів і на основі цього способу розробляється апаратно-програмний засіб внутрішньої охоронної системи комп'ютера та примусове розмежування доступу до носіїв інформації ПЕОМ.

Вибирається оптимальний спосіб машинозчитуємого латентного захисту, реалізований методом нанесення радіоактивної мітки (крапки) на носій інформації, вузол, прилад з наступним її зчитуванням.

Мітка являє собою радіоактивну речовину з визначеними наступними параметрами:

- вид випромінювання, енергія, активність, (максимально радіаційно безпечних, що майже не перевищують техногенний фон);
- радіонуклід;
- агрегатний стан і фізико-хімічні властивості речовини – носія радіонукліду;
- оптимальна поверхня і глибина знаходження мітки;

Слаборадіоактивна **мітка** для забезпечення фізичної безпеки **міцно поєднується:**

- з елементом, вузлом, приладом, матеріалом апаратної бази ПЕОМ;
- з носієм інформації (дискетою, пристроєм для мобільного використання жорсткого магнітного диску, з'ємним жорстким диском, пластиковою карткою тощо);
- із захищуваним вузлом, приладом КЗЗ щодо розмежування доступу, ідентифікації, автентифікації користувача ПЕОМ тощо.

Слаборадіоактивна мітка має не точно дозовану активність (мін. – мах.), на неї налаштована схема зчитування і контролю.

Схема зчитування і контролю схемно-апаратним способом включається в автономний процесор КЗЗ, який знаходиться на одній із шин AT, VLB, PCI та "епізодично" за програмою або "вибірково" контролює вузли зчитування і активність кожної мітки (мін. – мах.).

Автономний процесор захисту вибирається та програмується (створюються ліцензійно чисті програми керування роботою цього процесору) у відповідності з обраними політикою та моделлю фізичної безпеки КС. Після інсталяції системи захисту на ПЭОМ операції запису і зчитування на відповідних дисководах здійснюються тільки з маркованими носіями інформації, а при вилученні або заміні маркованих вузлів, фізичних елементів ПЕОМ, що захищена таким способом, видає інформацію щодо стану фізичної безпеки КС і стає непрацездатною.

Орієнтовний проект технічних вимог:

1. Об'єкт захисту – ПЕОМ типу IBM;
2. Захищувані пристрої – накопичувач на гнучких магнітних дисках, накопичувач на жорстких магнітних дисках; контроллери; блоки ОЗУ; " Мазерборт" тощо;
3. Спосіб захисту – використання слаборадіоактивної латентної машинозчитуваної мітки (крапки);
4. Радіоактивні ізотопи (РАІ) використовувати із групи Г (група мінімальної радіотоксичності);
5. Час зберігання радіоактивної мітки не менше 20 років;
6. Активність мітки вибрати оптимальною для виключення помилок першого та другого роду;
7. Використовувати малогабаритні детектори випромінювання (діаметром не більше 11 мм і довжиною не більше 36 мм);

8. Зберігання мічених носіїв інформації (РАІ) здійснюється у контейнерах по 10 штук, загальною кількістю приблизно 3000 шт., в локальному місці (приміщенні);

9. Реалізацію способу захисту здійснити спецпроцесором захисту, здатному працювати в автономному режимі і встановлюватися на одну із шин AT, VLB, PCI;

10. Спецпроцесор захисту має забезпечувати:

а) контроль робочих властивостей детекторів зчитування мітки;

б) контроль наявності радіоактивної мітки на носію інформації, вузлі, приладі (мін. – макс.);

в) дозвіл на роботу пристрою, що захищається, за наявності радіоактивної (РАІ) мітки на носію інформації та компоненті КЗЗ, що захищаються;

г) заборону на роботу пристрою, що захищається, при відсутності РАІ мітки на носію інформації та компоненті КЗЗ, що захищаються;

д) можливість підключення додаткових пристроїв захисту в ПЕОМ;

е) введення екстракодів (ЕК) санкціонованого доступу користувача (СДК) для зняття захисту вибраного пристрою:

ж) можливість зміни ЕК СДК;

з) індикацію наявності РАІ мітки на промаркованих матеріалах, елементах, вузлах, приладах та носіях інформації, компонентах КЗЗ і справності системи захисту.

12. Реакція спецпроцесору захисту для ідентифікації РАІ мітки на ГМД-3.5 – не більше 5 сек.;

13. Несанкціоноване вилучення (заміна) маркованих вузлів, детекторів реєстрації випромінювання блокує роботу ПЕОМ з видачею сигналу диспетчеру ТЗІ;

14. Несанкціоноване вилучення спецпроцесору захисту блокує роботу ПЕОМ;

15. Споживана потужність програмно-апаратного засобу – не більше 0,1 Вт.

IV Висновки

На основі викладеного вище можна зробити наступні висновки та рекомендації.

1. Забезпечення фізичної безпеки складових архітектури, елементної бази та носіїв інформації захищених комп'ютерних систем може бути успішно реалізовано, у тому числі, з використанням запропонованих способів захисту за допомогою радіоактивних міток.

2. Запропоновані способи захисту з використанням радіоактивних ізотопів екологічно безпечні, бо сумарна активність понад 50000 радіоактивних крапок-міток не перевищує мінімально визначену активність.

3. Інформація, викладена у статті, може бути корисна для теоретичного і практичного використання розглянутих способів та засобів для ефективного і надійного захисту складових КЗЗ КС та носіїв інформації: лазерних, гнучких та жорстких магнітних дисків, електронних карток тощо, а також використовувати радіоізотопи для експертних оцінок фізичної безпеки комп'ютерних систем, систем на стадіях від розробки до впровадження, експлуатації та модифікації.

4. Способи захисту можуть бути також реалізовані з метою латентного захисту інших об'єктів, наприклад, цінних паперів, документів, зброї, вузлів і деталей автомобілів, що підлягають обов'язковому контролю, ідентифікації, автентифікації тощо.

Література: 1 Деклараційний патент на винахід № 98031566."Спосіб захисту документів, цінних паперів та предметів, що мають історичну, художню цінність від підробок та викрадень методом радіоактивних індикаторів". Ю. І. Федоренко, І. І. Пающик, Г. Е. Массальський, А. Ю. Ільницький., О. Ф. Климюк. Держпатент України Бюл. № 8, 29.12.1999 р. 2. Деклараційний патент на винахід № 2000073954 "Спосіб прихованого символьнографічного щільнокодованого радіоізотопного захисту носіїв інформації, предметів та пристрій зчитування для реалізації цього способу" І. І. Пающик, Держпатент України Бюл. № 8, 17.09.2001. 3. НД ТЗІ 2.5-004-99 Департаменту СТСЗІ СБУ. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. В. В. Шорошев, А. Е. Ильницкий, И. Л. Близнюк – К., 1999. 4. Защита информации компьютерных систем от угроз НСД и национальные критерии ее экспертной оценки. В. В. Шорошев, Бизнес и безопасность № 6, – К., 2000.