УДК 004.9+681.3+655.5

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ВІД АТАК НА RFID-МІТКИ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОБЛІКУ КНИЖКОВОЇ ПРОДУКЦІЇ

Р. О. Козак[1], Н. І. Яворська[2], А. В. Яворський[2], О. І. Осінчук[1]

[1]Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна

[2]Тернопільський національний технічний університет імені Івана Пулюя,
вул. Руська, 56, Тернопіль, 46001, Україна

Розглянуто переваги застосування технології RFID-ідентифікації, проаналізовано загрози інформаційній безпеці та потенційні атаки на ідентифікатори на основі RFID, описано підхід для підвищення рівня захисту інформації, яка ідентифікує книжкову продукції в системах обліку, перелічено способи підвищення стійкості RFID-систем.

Ключові слова: *захист інформації, RFID-мітка, інформаційна безпека, облік книжкової продукції, ризики інформаційної безпеки.*

Постановка проблеми. Для будь-якої торгової мережі однією з найбільш збиткових ситуацій є пограбування. Крадіжку може здійснювати як стороння особа, так і співробітник торгової точки. В середньому за статистикою в категорії магазинів супермаркет/гіпермаркет рівень злодійства і втрат становить 1,6 % від товарообігу. Лідерами ж за рівнем втрат є магазини, що торгують книгами і листівками, музичними та відеозаписами, де рівень злодійства досягає в середньому 2,3 % від товарообігу [1]. Очевидно, що питання захисту товарів від крадіжки або підміни стає дедалі актуальнішим.

Аналіз останніх досліджень та публікацій. Нині галузь застосування інформаційних систем на основі технології RFID досить широка, особливо в сфері автоматизації бізнес-процесів, де відбувається процес послідовного заміщення технології штрихового кодування. Це пов'язано з тим, що RFID-системи мають значно більше переваг порівняно з традиційними системами штрихового кодування. Серед основних переваг технології радіочастотної ідентифікації можна виділити такі [2]:

- можливість дистанційного зчитування інформації з радіочастотних міток (допустима відстань від зчитувача до радіочастотної мітки залежить від застосовуваного частотного діапазону і може досягати десятків метрів);
- можливість зчитування радіочастотних міток, які перебувають всередині радіопрозорої упаковки, що дає змогу швидко визначати вміст пакувальних одиниць (коробок, ящиків тощо) без їх розкриття;
- можливість швидкого зчитування інформації з великої кількості радіочастотних міток, що дає змогу швидко визначати вміст пакувальних одиниць навіть в

разі, коли всередині упаковки є велика кількість маркованих виробів, причому ці вироби можуть бути як однаковими, так і різними;
- відсутність жорстких вимог з точності позиціонування щодо зчитувача і з просторової орієнтації радіочастотних міток, що спрощує автоматизацію процесу зчитування (антени зчитувача у разі потреби можуть бути розташовані у воротах, дверних отворах, в спеціальних порталах або в портативних RFID-зчитувачах);
- можливість дистанційного запису і перезапису інформації в радіочастотних мітках;
- можливість використання радіочастотних міток не тільки для автоматизованого обліку маркованих виробів, а й для виявлення їх несанкціонованого переміщення, зокрема розкрадання;
- можливість маркування не тільки номенклатури продукту, а й присвоєння унікального номера кожній одиниці продукту зі зберіганням інформації про технологічний процес виробництва і транспортування.

Мета статті — розглянути способи забезпечення захисту від атак на ідентифікатори на основі RFID-технології (Radio Frequency IDentification — радіочастотна ідентифікація), що застосовуються в системах обліку книжкової продукції. Радіочастотні мітки за своєю конструкцією укладаються в загальну схему побудови універсальних обчислювальних пристроїв, відрізняючись безконтактними інтерфейсами взаємодії з оточуючими їх елементами і зовнішнім середовищем. Це сприяє постійному розширенню сфери застосування RFID систем і появи нових поглядів на розвиток і способи використання інформаційно-телекомунікаційних систем. Поряд із зазначеними перевагами, сучасні системи радіочастотної ідентифікації різного рівня складності мають і деякі обмеження. RFID-системи містять досить широкий спектр бездротових пристроїв різної функціональності, потужності та складності, що дає змогу їх віднести до класу складних систем автоматизації з пред'явленням відповідних вимог щодо забезпечення захисту від несанкціонованого доступу до інформації. Захист даних і збереження інформації, що циркулює в радіочастотної системі, є питанням, яке набуває життєво важливого значення для ділової практики і затребуваності технології.

Виклад основного матеріалу дослідження. Із розвитком і поширенням безконтактних інформаційно-телекомунікаційних систем йде масштабне наростання загроз інформаційній безпеці, що проникають в глибші рівні обробки даних, тому при моделюванні та розробці радіочастотних систем особливу увагу потрібно приділяти питанням захищеності інформаційного середовища і розробці системи захисту інформації. Обов'язковим елементом розробки RFID-систем стає аналіз потенційних загроз і забезпечення захисту інформації на фізичному рівні обробки даних, захист елементів RFID-систем від фальсифікації, підробки і несанкціонованих дій, а також забезпечення інформаційної безпеки і розвантаження логічного (інформаційного) рівня обробки від експоненціально наростаючого числа транзакцій і великого потоку інформації, очікуваного і йде з фізичного рівня обробки даних, в міру розвитку і поширення безконтактних інформаційно-

телекомунікаційних систем [6]. У рамках проблеми захисту інформації в RFID-системах вирішуються такі завдання: забезпечення конфіденційності та автентифікації.

Забезпечення захисту товарів від крадіжки або підміни, засноване на системах, що складаються лише з голограм або мікродруку, нанесених на упаковку товару, має низку проблем, пов'язаних з тим, що позначки не приєднані безпосередньо до товару. Зв'язок між ними часто забезпечується тільки за допомогою сполучного з'єднання і може бути не досить надійним, тому не можна говорити про справжність товару лише на основі достовірності мітки, яка прикріплена до нього [3].

На відміну від перерахованих технологій, RFID-системи можуть ефективно вирішити цю проблему. Навіть бюджетні RFID-мітки з вельми обмеженим обсягом пам'яті можуть зберігати спеціальні дані про об'єкт (СДО), наприклад, точну вагу товару, його форм-фактор і навіть спектрографічний аналіз поверхні для посвідчення того, що RFID-мітка дійсно прикріплена до відповідного товару. Цей підхід нагадує використання особистих фотографій у паспортах, які логічно пов'язують документи з їх власниками. У результаті подібної системи захисту відсутня можливість видалення RFID-мітки у справжнього товару, а також її повторного застосування у підробленому товарі. Подібна RFID-система використовує спеціальні дані про об'єкт, що забезпечує необхідну надійність прикріплення між RFID-міткою і товаром, до якого вона прикріплена. RFID-система складається з чотирьох основних складових (рис. 1):

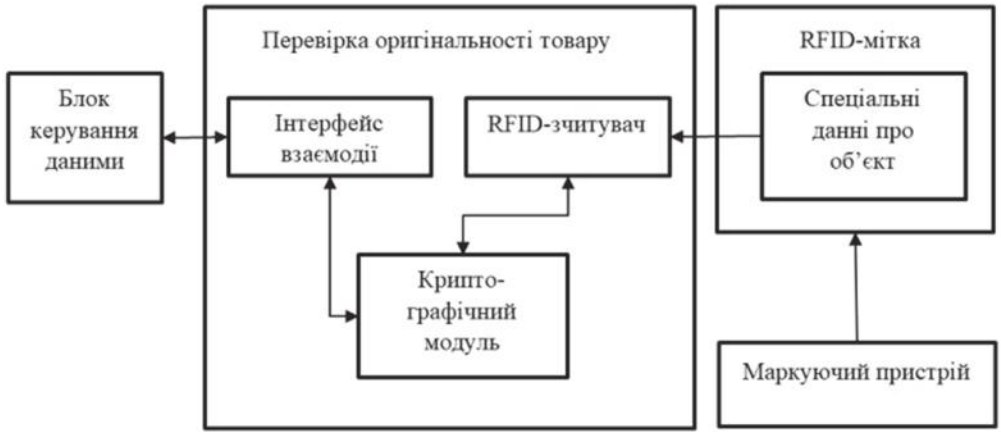

Рис. 1. Структура RFID-системи

– мітка, що містить спеціальні дані про об'єкт;
– маркуючий пристрій;
– блок керування даними;
– користувацький термінал [3].

Для зазначеної RFID-системи підходять пасивні RFID-мітки (позбавлені джерела енергії; електричний струм в подібних мітках індукується в антені

електромагнітним сигналом від зчитувача) з ємністю для зберігання даних від 32 до 64 байт. Водночас в мітках не вимагається виконання криптографічних функцій, вони лише зберігають спеціальні дані про об'єкт.

Дані про справжність товару:

– унікальний номер мітки;
– унікальний серійний номер товару;
– специфічні дані товару;
– метод підпису;
– значення підпису.

RFID-мітка містить унікальний номер, який програмує виробник мітки в процесі її виробництва. Унікальний серійний номер товару — це номер, який призначає власник торгової марки. Номер може ґрунтуватися на системі нумерації Європейської Патентної Конвенції (ЄПК) [4] або будь-якій інший системі нумерації, яка полегшує ідентифікацію унікальних об'єктів. Дані, які характеризують окремий товар, зокрема книжкову продукцію, не змінюються з плином часу і легко вимірюються під час огляду. Дані мають бути унікальні з того погляду, що два різних примірника того самого товару можуть бути помічені за допомогою характерної риси, наявної в описі. Вибір властивостей залежить від особливих вимірюваних характеристик, таких як фізичні, хімічні, електричні та інші, які має певний товар і які доступні для вимірювального устаткування. Наведемо як приклад характеристики, що або повністю, або частково описує товари: маса, фізичні розміри, серійний номер, надрукований на товарах або їх упаковці тощо. Ці дані зазвичай записує в RFID-мітки постачальник товару перед його постачанням, наприклад, в процесі упаковки. Також можна зберігати посилання на дані про RFID-мітки, наприклад, уніфікований ідентифікатор ресурсу (URI), які точно визначають запис у віддаленій базі даних. Це допомагає скоротити ємність RFID-мітки і у такий спосіб дасть змогу застосовувати дешевші мітки, але проведення перевірки товару залежить від наявності мережевого з'єднання.

Послідовність бітів, яка визначає комбінацію криптографічних методів, використовуваних під час обчислення значення підпису називається підписом. Ця інформація використовується на терміналі для застосування потрібного криптографічного алгоритму під час перевірки достовірності товару. Значення підпису: постачальник товару обчислює значення підпису, використовуючи криптографічний хеш-функцій *h* з асиметричним шифруванням *SPr*. Значення підпису = *SPr* (*h* — унікальний номер мітки, унікальний серійний номер товару, специфічні дані товару, метод підпису, значення підпису).

Обчислюючи значення підпису, *SPr* використовує секретний ключ продавця товару (ключ підпису), який має бути відомий лише йому. Для перевірки справжності значення підпису використовується відкритий ключ (ключ перевірки). Кріплення пасивної RFID-мітки на товар здійснюється за допомогою так званого маркуючого пристрою, який відповідає за вимір спеціальних даних про об'єкт і запис результатів на мітку і в базу даних виробника. Блок управління даними зберігає спеціальні дані про об'єкт і полегшує управління доступом. Принцип

роботи блоку управління даними схожий з системою, що займається лише перевіркою достовірності серійних номерів, за винятком того, що кожен запис бази даних збільшується завдяки додатковій інформації про товари (СДО).

Термінал (по суті, пристрій, що контролює справжність товарів) складається з модуля зчитування, пристрою вимірювання СДО, обчислювального модуля, інтерфейсу користувача і засобу мережевого з'єднання. Модулем зчитування може бути будь-який пристрій, що має можливість зчитувати СДО за певними адресами пам'яті. Обчислювальний модуль відповідає за перевірку цілісності СДО, тобто пристрій перевіряє, чи була змінена інформація в RFID-мітці, для того щоб своєчасно проінформувати про можливу підробленого запису в базі даних. Засіб створення мережевого з'єднання необхідний для знаходження відкритого ключа через довірене джерело виробника товару. В альтернативному випадку користувач може також зберігати необхідні секретні ключі, які дають змогу перевірити товар без підключення до мережі. Перевага такого підходу полягає в тому, що можуть бути використані бюджетні пасивні RFID-мітки з ємністю для зберігання даних всього 32–64 байт. При цьому в мітках не потрібно застосування криптографічних функцій, які необхідні для більш дорогих RFID-міток.

Описаний підхід також може бути комбінований з перевіркою достовірності, яка ґрунтується на відстеженні переміщення або правилах ідентифікації захищених RFID-міток з метою запобігання їх копіювання або видалення з справжньої RFID-системи [5]. Отже, метод успішно запобігає атаки, метою яких є підміна або видалення RFID-міток, закріплених на товарах. Метод підходить для бюджетних RFID-міток, які повсюдно використовуються в різних сферах і галузях. Мітка, прикріплена до об'єкта і жорстко пов'язана з ним, містить спеціальні дані про цей об'єкт.

Описана RFID-система дає змогу виміряти об'єкт, що допомагає уникнути копіювання. Це рішення також придатне для перевірки достовірності товару без наявності підключення до мережі або у випадках, якщо мережа недоступна. Недолік методу полягає в тому, що він застосовується лише в тому випадку, якщо захищаються товари які мають особливі унікальні властивості, які можуть бути перевірені економічно вигідним способом. Особливими унікальними властивостями товару, зокрема книжкової продукції, можуть бути не тільки індивідуальні особливості, але також інформація з електронних документів на вантаж і митних декларацій, вага партії, інформація про джерело і пункт призначення, дата відвантаження і тому подібні відомості можуть слугувати як спеціальні дані про об'єкт для прив'язки документів до певного товару.

Системи радіочастотної ідентифікації, побудовані на базі технології EPCglobal, схильні до атак, пов'язаних з перехопленням електромагнітних випромінювань між зчитувачем і міткою, а так само з доступом до інформації, що міститься на радіочастотній мітці, або її компрометацією. Основна загроза може виходити від порушника, оснащеного високотехнологічними радіочастотними засобами і стандартним лабораторним контрольно-вимірювальним обладнанням, за допомогою якого відбувається «прослуховування» авторизованої операції зв'язку між зчитувачем і

радіочастотною міткою. За допомогою подібного обладнання можлива організація DoS-атак (атак, що викликають відмову в обслуговуванні) на інфраструктуру радіочастотної системи через наповнення діапазону 860-930 МГц, що використовується для радіочастотних міток стандарту EPC Gen2, шумовими перешкодами або використанням великої кількості фіктивних радіочастотних міток. Подібна атака може привести як до тимчасової втрати працездатності системи через технологічні обмеження, пов'язані з неможливістю опрацювання одноразово великої кількості радіочастотних міток, так і до тривалої відмови в обслуговуванні, що виходить від RFID зчитувачів [6].

Друга група можливих атак пов'язана з відсутністю захисту інформації, записаної на радіочастотну мітку. Існуючий рівень забезпечення безпеки, реалізований в протоколі EPC Gen2, дає змогу розробникам RFID-систем обмежити доступ до функціональних команд радіочастотної мітки, за допомогою яких радіочастотна мітка може бути повністю дезактивована або її EPC номер (унікальний ідентифікатор об'єкта) може бути прихований за допомогою захисту їх 32-розрядними паролем, який може виступати як базовий рівень захисту радіочастотних міток. На жаль, подібний метод захисту інформації має низку вразливостей:

1. Під час роботи з радіочастотної міткою пароль передається у відритому вигляді і може бути отриманий через прослуховування каналу зв'язку.
2. Використовуючи атаки, засновані на аналізі потужності випромінювання, є змога виявляти пароль, оскільки мітка в процесі автентифікації використовує різний рівень потужності сигналу, що залежить від того, наскільки кожен наступний біт відповідає значенню чинного пароля.

Для підбору ключа можна використовувати спрямовану антену і цифровий осцилограф. При надсиланні на чіп невірного біта ключа шифру, використовуючи 8- і 32-бітове шифрування даних, енергоспоживання інтегральної мікросхеми зростає і радіочастотна мітка випромінює менше енергії, на відміну від випадку, коли біт ключа справджується, що може бути легко зафіксовано. Використовуючи цей метод, злом досить довгих ключів за фіксований час стає можливим, що неможливо при використанні методів підбору пароля.

Отже, зловмисник може отримати конфіденційну інформацію про об'єкт ідентифікації за допомогою фізичної атаки, змінити дані, сформувати потрібну кількість копій або деактивувати радіочастотні мітки. Під час отримання зловмисником доступу до зміни інформації, що міститься на радіочастотній мітці, цілком можливий запис шкідливих даних, за допомогою яких можливе здійснення таких атак, як SQL-ін'єкція або переповнення буфера, успішна реалізація яких може призвести до порушень в роботі та надання доступу до RFID- системи третім особам [6-8].

Отже, більшість загроз може бути реалізовано під час впливу на радіоканал з метою маніпуляції даними, переданими по цьому каналу, що призведе до порушення працездатності системи, зокрема до порушення зв'язку між зчитувачем і радіочастотними мітками, блокування інформації. З цими загрозами можна боротися, використовуючи криптографічні протоколи обміну інформацією, побудовані на асиметричних алгоритмах з відкритим ключем, і шифрування даних,

що зберігається. Однак наділення радіочастотних міток подібними функціями потребує додаткових обчислювальних ресурсів і розширеної незалежної пам'яті, що призведе до ускладнення і, як наслідок, підвищення вартості міток.

У випадку з пасивними мітками, до яких належать радіочастотні мітки технології EPCglobal, може виникнути ситуація, коли необхідної енергії, одержуваної антеною радіочастотної мітки від зчитувача, не вистачить для виконання подібних операцій і буде потрібна розробка спеціальних рекомендацій для забезпечення високої надійності та працездатності радіочастотної системи. Такі обмеження пасивних міток можуть стати серйозною перешкодою для використання та впровадження RFID-систем.

Як бачимо, рівень захисту інформації, реалізований в стандартах EPC Gen2, не є достатнім для задоволення сучасних вимог до захисту даних, і надає можливості для здійснення атак, описаних вище. У зв'язку з цим розробники систем для зниження ризиків несанкціонованого доступу до даних змушені керуватися рекомендаціями щодо посилення захисту інформації радіочастотної системи загалом.

Рекомендованими є такі способи підвищення стійкості RFID-систем до перерахованих вище загроз:

1. *Мінімізація конфіденційних даних на мітці.* Цей спосіб ґрунтується на перенесенні даних з пам'яті радіочастотної мітки в надійне сховище даних інформаційно-керуючої системи організації і використанні унікального ідентифікатора або EPC-номера мітки як ключа доступу до цих даних. На жаль, цей підхід не виключає можливості отримання зловмисником цінної інформації і від одного ідентифікатора. Наприклад, знаючи структуру EPC, можна виявити мінімальну інформацію про об'єкт ідентифікації.

2. *Парольний захист радіочастотних міток.* Сучасні радіочастотні мітки вже мають у своєму розпорядженні достатні технічні ресурси для верифікації за допомогою пароля, який вже став невід'ємною частиною комплексу рішень для захисту даних. Радіочастотна мітка не дозволить виконати захищені паролем команди на читання, запис, деактивацію або на доступ до захищеної ділянки пам'яті, якщо вони не супроводжуються правильним паролем. Водночас в традиційних інформаційних системах відбувається періодична зміна паролів, в RFID-системах подібні зміни можуть бути неможливими через те, що радіочастотні мітки часто не доступні для процесу призначення паролів. У зв'язку з цим гарним вибором буде призначення різних паролів для кожної мітки і кожної області даних всередині мітки, що істотно збільшить кількість необхідних ресурсів на компрометацію паролів. Подібний підхід вимагає використання бази даних, що містить паролі, прив'язані до ідентифікаторів міток. Можливий також підхід з використанням деякого секретного алгоритму генерації паролів на основі унікального ідентифікатора мітки, що звільняє організацію (розповсюджувача книжкової продукції) від зберігання і супроводу баз даних з паролями.

3. *Шифрування даних.* Шифруванням можливе забезпечення надійного захисту збережених і переданих відкритими каналами даних. Шифрування не виключає зовнішніх загроз, пов'язаних з фізичним стеженням і проникненням в радіоканали зв'язку, але значно ускладнює завдання для зловмисника [4].

4. *Підписування даних.* Підписування інформації, що міститься на радіочастотній мітці, електронним цифровим підписом дає змогу виключити з участі в інформаційному обміні RFID-системи як копії міток, так і міток зі зміненими зловмисником даними. Цей спосіб заснований на додаванні незмінного унікального ідентифікатора радіочастотної мітки до інформації, що міститься на радіочастотній мітці, з подальшою генерацією деякої цифрового підпису за допомогою приватного ключа. Цифровий підпис зберігається разом з даними на радіочастотні мітці та перевіряється за допомогою відкрито розповсюджуваного публічного ключа. У цій схемі важливим фактором є отримання публічного ключа перевірки підпису з достовірного джерела.

5. Забезпечення фізичного захисту RFID-систем. Такий підхід дає змогу забезпечити захист від фальсифікації даних або генерації перешкод в роботі RFID-системи через реалізацію заходів щодо забезпечення електромагнітного екранування місця роботи радіочастотної системи або через зменшення потужності зчитувача і, як наслідок, відстані зчитування в ланцюжку зчитувач — радіочастотна мітка.

Висновки. Наявні можливості технології радіочастотної ідентифікації та використання описаного вище комплексу заходів щодо забезпечення захисту інформації RFID-систем дають змогу зробити висновок, що сучасний стан галузі RFID можна охарактеризувати як фазу зрілого вдосконалення. Незважаючи на актуальність питань захищеності пасивних радіочастотних міток, які потребують розробки спеціальних технічних рішень, запропонований розробниками EPCglobal функціонал, що забезпечує захист даних, спільно з класичними підходами захисту інформації в інформаційних системах, характеризується керованими ризиками і може застосовуватися для розробки RFID-систем.

Однак, незважаючи на всі переваги радіочастотних систем, потрібно визнати існування реальної загрози конфіденційності, що обмежує область застосування таких систем, зокрема для обліку книжкової продукції. У зв'язку з цим зацікавлена у впровадженні RFID-систем мережа збуту має використовувати різні методи захисту та управління системою захисту інформації, оперативного і технічного контролю для нівелювання ризиків, що виникають під час впровадження RFID-систем. Необхідно враховувати, що кожне конкретне впровадження RFID-системи нерозривно пов'язано зі специфікою виконуваних завдань і не всі чинні сьогодні методи захисту можуть бути ефективні в розглядуваній галузі. Насамперед необхідно оцінити ризики, пов'язані з впровадженням RFID-технології і виробити відповідні рішення щодо забезпечення контролю та застосування методів захисту інформації, зважаючи на всі можливі фактори, такі як: величина загроз, вартість впровадження і забезпечення технічної підтримки, а такаж продуктивність системи і можливі збитки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Крамарєв А. Н. Найбільша проблема роздрібної торгівлі 21 століття. Санкт-Перетбург: НОУ Інститут проблем підприємництва, 2004. URL: http://www.ippnou.ru/article.php?idarticle=000423.

2. Організація протидії технічним засобам розвідки в автоматизованих системах управління з елементами радіочастотної ідентифікації / Васильєв С. В., Сілкін А. Т., Тікменова І. В., Уткін А. В. Науково-методичні матеріали досліджень, праці семінарів і науково-технічних конференцій 3 ЦНДІ МО РФ. Книга 12. Москва: 3ЦНІІ МО РФ, 2008. С. 38–41.
3. Nochta Z., Staake T., Fleisch E. 2006. Product specific security features based on RFID technology. In Proceedings, International Symposium on Applications and the Internet Workshops – SAINTW ‘06. Pp. 72–75.
4. European Patent Convention. European Patent Office. URL: http://www.epo.org/law-practice/legal-texts/html/epc/2010/e/index.html.
5. Севастьянова Б. А. Зроблені шифри: Вступне слово чл.-кор. РАН Москва: Геліос АРВ, 2003. 160 с. Іл. С. 11–16.
6. Sarma Sanjay E., Weis Stephen A., Engels Daniel W. RFID Systems and Security and Privacy Implications, Auto-ID Center, Massachusetts Institute of Technology, Cambridge, MA 02139. B. S. Kaliski Jr. et al. (Eds.): CHES 2002 LNCS 2523. 2003. Pp. 454–469.
7. Maricel O. Balitanas and Taihoon Kim Review: Security Threats for RFID-Sensor Network Anti-Collision Protocol. International Journal of Smart Home. 2010. Vol. 4. № 1. January. Pp. 23–36.
8. Liang Y., Rong C. Strengthen RFID Tags Security Using New Data Structure. International Journal of Control and Automation. 2008. Vol. 1. № 1. Pp. 51–58.

REFERENCES

1. Kramariev, A. N. (2004). Naibilsha problema rozdribnoi torhivli 21 stolittia. Sankt-Peretburh: NOU Instytut problem pidpryiemnytstva. Retrieved from http://www.ippnou.ru/article.php?idarticle=000423 (in Ukrainian).
2. Vasyliev, S. V., Silkin, A. T., Tikmenova, I. V., & Utkin, A. V. (2008). Orhanizatsiia protydii tekhnichnym zasobam rozvidky v avtomatyzovanykh systemakh upravlinnia z elementamy radiochastotnoi identyfikatsii. Naukovo-metodychni materialy doslidzhen, pratsi seminariv i naukovo-tekhnichnykh konferentsii 3 TsNDI MO RF. Knyha 12. Moskva: 3TsNII MO RF, 38–41 (in Ukrainian).
3. Nochta, Z., Staake, T., & Fleisch, E. (2006). Product specific security features based on RFID technology. In Proceedings, International Symposium on Applications and the Internet Workshops – SAINTW ‘06., 72–75 (in English).
4. European Patent Convention. European Patent Office. Retrieved from http://www.epo.org/law-practice/legal-texts/html/epc/2010/e/index.html (in English).
5. Sevastianova, B. A. (2003). Zrobleni shyfry: Vstupne slovo chl.-kor. RAN Moskva: Helios ARV (in Ukrainian).
6. Sarma, Sanjay E., Weis, Stephen A., & Engels, Daniel W. (2003). RFID Systems and Security and Privacy Implications, Auto-ID Center, Massachusetts Institute of Technology, Cambridge, MA 02139. B. S. Kaliski Jr. et al. (Eds.): CHES 2002 LNCS 2523., 454–469 (in English).
7. Maricel, O. (2010). Balitanas and Taihoon Kim Review: Security Threats for RFID-Sensor Network Anti-Collision Protocol: International Journal of Smart Home, Vol. 4, 1, January, 23–36 (in English).
8. Liang, Y., & Rong, C. (2008). Strengthen RFID Tags Security Using New Data Structure: International Journal of Control and Automation, Vol. 1, 1, 51–58 (in English).

doi: 10.32403/1998-6912-2018-2-57-54-63

PROTECTION METHODS AND APPROACHES AGAINST RFID-ATTACKS IN AUTOMATED REGISTRATION SYSTEMS OF BOOK PRODUCTS

R. O. Kozak[1], N. I. Yavorska[2], A. V. Yavorsky[2], O. I. Osinchuk[1]

[1]Ukrainian Academy of Printing,
19, Pid Holoskom, St., Lviv, 79020, Ukraine

[2]Ternopil Ivan Puluj National Technical University,
56, Ruska, St., Ternopil, 46001, Ukraine
ruslan.o.kozak@gmail.com

The advantages of using RFID-identification technology have been analyzed. The available capabilities of radio frequency identification technology and the use of the above-mentioned set of measures to ensure the protection of RFID-systems information allow us to conclude that the current state of RFID industry can be characterized as a phase of mature improvement. In spite of all the benefits of radio frequency systems, the existence of a real threat of confidentiality, which limits the scope of such systems, in particular for the registration of book products, should be recognized.

Information security threats and potential attacks on identifiers based on RFID have been discovered. The sales network interested in the implementation of RFID systems should use different methods of protection and management of the information security system, operational and technical control to minimize the risks arising from the introduction of RFID systems. An approach to increase the level of information security that identifies book products in registration systems has been described. It should be borne in mind that each specific implementation of the RFID system is inextricably linked with the specifics of the tasks performed, and not all current methods of protection can be effective in the industry. It is necessary to evaluate the risks associated with the implementation of RFID technology and to develop appropriate solutions to ensure the control and application of information protection methods, taking into account all possible factors such as: the magnitude of the threats, the cost of implementation and technical support, and also the performance of the system and possible losses. The ways of increasing the stability of RFID systems have been listed. System developers to reduce the risks of unauthorized access to data are forced to follow the recommendations for strengthening the protection of information of the radio frequency system in general. The following methods are recommended to improve the stability of RFID systems to the above threats: minimize the confidential data on the label, password protection of radio frequency tags, data encryption, data signing, and the physical protection of RFID systems.

Keywords: *information security, RFID tag, book inventory, information security risks, security threats.*

Стаття надійшла до редакції 25.06.2018.
Received 25.06.2018.