УДК 004.056.53 (045)

ПРОТИДІЯ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ЗНІМНІ НОСІЇ

А. Б. Петренко, канд. техн. наук, доц.; ***Є. В. Бєтанов***

Національний авіаційний університет

betanovev@ukr.net

Запропоновано розроблення програмного продукту, що здійснюватиме контролювання підключення зовнішніх пристроїв накопичування даних, а також виконуватиме криптографічні перетворення інформації з використанням ідентифікатора середовища зберігання даних. Розроблені та описані алгоритми було реалізовано на практиці та будуть тестованні.

Ключові слова: захист інформації, внутрішні загрози, зовнішні носії, несанкціоноване підключення, криптографічне перетворення, алгоритм.

In this article authors justified and formed task to develop the software for monitoring of connection external devices to computer system. Software also will make cryptographic transformation of information using an identifier of storage environment. Developed and described algorithms were also implemented in practice and tested.

Keywords: information security, internal threats, external devices unauthorized connections, cryptographic transformation, algorithm.

Вступ

Мета системи захисту — зберегти такі властивості інформації як цілісність, спостережність, доступність та достовірність. Кожній системі захисту притаманна наявність слабких місць, що призводять до утворення каналів витоку інформації. Загалом, усі загрози інформаційній безпеці можна поділити на внутрішні та зовнішні.

Найслабкішим місцем систем захисту електронної інформації є внутрішні загрози. Проведені дослідження щодо співвідношення внутрішніх та зовнішніх загроз подано на рис. 1.

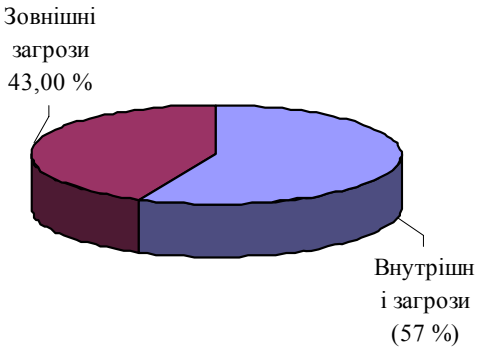

Рис. 1. Співвідношення внутрішніх та зовнішніх загроз

Здебільшого дії персоналу, що має безпосередній легальний доступ до автоматизованої системи (АС), контролюються нормативними та організаційними заходами. Але при спробі здійснення несанкціонованого доступу їх буде замало.

Користувач який має безпосередній легальний доступ до автоматизованої системи, може реалізувати такі загрози:

– здійснити *крадіжку конфіденційної інформації* — користувач може скопіювати інформацію на портативні пристрої, чи на зовнішні носії, опублікувати її на веб-сайті, відправити за помилковим поштовим індексом. Може реалізовуватися через помилку користувача або через його навмисні дії;

– порушити *авторські права на інформацію* — здійснення несанкціонованого копіювання авторського документу чи його частини, шифрування документу з власним паролем, підробка реквізитів іншого користувача чи компанії. Найчастіше реалізується через навмисні дії користувачів;

– *шахрайство* — спотворення фінансової документації, перевищення повноважень під час роботи з базами даних, модифікація важливих даних. Реалізується через навмисні дії задля досягнення певної мети;

– *саботаж інформації* — реалізується навмисно задля досягнення певної мети чи для помсти.

Проаналізувавши можливості з утворювання користувачами каналів витоку інформації, можна перелічити їх у порядку зменшення ймовірності реалізації (рис. 2):

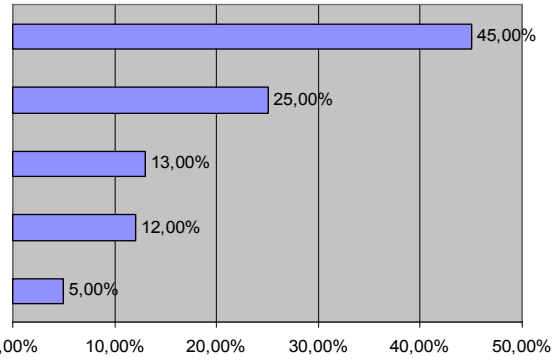

Рис. 2. Імовірність реалізації внутрішніх каналів витоку інформації

- зовнішні носії — 45 %;
- пересилання файлів мережею Internet — 25 %;
- друк файлів на принтері — 13 %;
- фотографування документів на цифрові камери — 12 %;
- інші — 5 %.

Аналіз досліджень та публікацій

Проаналізовані джерела виділяють внутрішні загрози як основну причину спричинення каналу витоку інформації [1; 2].

У свою чергу, зовнішні пристрої накопичування даних є головним засобом здійснення витоку інформації через її копіювання самим користувачем для подальших неправомірних дій із нею [3].

Для попередження витоку інформації через її копіювання на зовнішні пристрої накопичування даних пропонується повне блокування USB портів вводу/виводу інформації [4].

У запам'ятовуючих пристроях міститься унікальний ідентифікатор [5], за яким можна проводити перевірку пристрою, що підключається до комп'ютера. Тому авторами були опубліковані матеріали, направлені на поліпшення системи захисту електронної інформації через ідентифікацію знімних носіїв, що підключаються через інтерфейс USB [6—10].

Постановка проблеми

Для реального здійснення попередження неправомірних дій з інформаційними ресурсами необхідно обмежувати дії авторизованого користувача зі здійснення підключення незареєстрованих пристроїв, а також контролювати розповсюдження важливої інформації, що знаходиться на його знімних носіях.

На даний момент існують програмні комплекси із забезпечення захисту електронної інформації від витоку внутрішніми та зовнішніми каналами. Ці засоби зазвичай регламентують дії користувача шляхом встановлення політик безпеки, що обмежують його повноваження під час роботи з інформацією.

Стосовно зовнішніх носіїв, їх використання регламентується забороною їх підключення, редагуванням налаштувань операційної системи. Але посадові обов'язки користувача зазвичай потребують можливості швидкого копіювання документів на знімні носії.

Таким чином, авторами було поставлено завдання розробити програмний продукт, що обмежуватиме використання запам'ятовуючих пристроїв. При цьому користувачеві можна виділити пристрої, робота з якими буде дозволена.

Додатково буде розроблено модуль, що здійснюватиме шифрування тексту на зовнішньому носії з використанням його ідентифікатора як частини ключа.

Актуальність тематики полягає в широкому розповсюдження зовнішніх пристроїв накопичування даних, а отже, розробки з вдосконалювання системи використання цих пристроїв будуть доречними.

Викладення основного матеріалу

У запам'ятовуючих пристроях АС, як правило, міститься інформація про конфігурацію пристрою. До такої інформації належать: типи пристроїв та їх характеристики, режими роботи й інша інформація.

За допомогою програмних засобів може бути організований збір і порівняння інформації про конфігурацію пристрою.

Ще більш надійний та оперативний метод контролю — використання спеціального коду-ідентифікатора пристрою.

Цей код може генеруватися апаратними засобами, а може зберігатися в запам'ятовуючих пристроях.

Генератор може ініціювати видачу в контролюючий пристрій (в обчислювальній мережі це може бути робоче місце адміністратора) унікального номера пристрою.

Код із запам'ятовуючого пристрою може періодично зчитуватися і аналізуватися засобами адміністратора комп'ютерної системи.

Було розроблено програмний продукт, що блокує зовнішні пристрої накопичування даних з інтерфейсом підключення USB. Блокування даних пристроїв зумовлено їх компактними габаритами, дешевими цінами та широкою доступністю, засоби обчислювальної техніки підтримують обмін інформацією за цією технологією.

Програмний продукт відслідковує підключення зовнішніх носіїв, і при спробі підключення будь-якого пристрою виконує такі дії.

– перевіряє чи є дозвіл на використання цього пристрою у певного користувача;

– якщо дозволу немає — блокує цей пристрій, якщо дозвіл є — дозволяє користувачу працювати з цим пристроєм;

– блокування проводиться у два етапи: вимкнення пристрою, блокування USB портів;

– при блокуванні видається візуальний сигнал тривоги;

– дає можливість розблокувати порти адміністратору системи після введення ним персонального паролю.

При розробці програми були реалізовані такі елементи:

– функція, що відслідковує підключення та перевірку носіїв;

– база даних, де зберігаються ідентифікатори носіїв, якими дозволено користуватися;

– система управління базою даних, яка дозволяє додавати, видаляти чи редагувати інформацію про пристрої та їх власників;

– система адміністрування, що не дозволяє не санкціоновано змінити базу даних, вимкнути програму, розблокувати порти;

– додаткового захисту пристроїв паролями користувачів.

Алгоритм роботи програми складається з кількох базових етапів:

– алгоритм моніторингу портів та перевірки підключених пристроїв.

– алгоритми адміністрування.

Перший алгоритм викликається з інтервалом у три секунди. Він призначений для виконання захисту системи від підключення незареєстрованих пристроїв. При цьому відслідковується зміна у змінній, що відповідає за збереження літер, які відповідають міткам підключених томів.

Том — частина довготривалої пам'яті комп'ютера, тобто всі пристрої, що мають пам'ять (локальні диски, CD/DVD-ROM, USB флеш-пристрої, дискети, переносні вінчестери і навіть мобільні телефони).

Алгоритми адміністрування — абстракція що складається з кількох підрозділів.

Моніторинг ключових подій та перевірка в суб'єкта прав на їх виконання.

До ключових подій належать: перехід з режиму моніторингу системи до адміністрування бази даних, вимкнення програми, блокування / розблокування портів. Ці дії потребують введення паролю адміністратора.

Виконання допоміжних функцій: встановлення паролю користувача, зміна паролю адміністратора, адміністрування бази даних. Останні дві функції знаходяться в режимі роботи з правами адміністратора.

Алгоритм моніторингу портів та перевірки підключених пристроїв наведено на рис. 3.

Другим, важливим компонентом програмного продукту є можливість надати користувачеві гарантії, що при викраденні інформації з середовища її зберігання, вона не буде доступна зловмиснику.

Для цього був розроблений алгоритм, який формує ключ шифрування на основі ідентифікатора пристрою накопичування даних і передає його в алгоритм криптографічного перетворення. Даний алгоритм дає змогу шифрувати інформацію з використанням ідентифікатора фізичного середовища: жорсткі диски, флеш-накопичувачі тощо.

При розшифруванні система зробить запит на введення паролю користувача, а також на отримання ідентифікатора пристрою, на якому збережено файл. При копіюванні інформації з середовища її зберігання і спробі розшифрувати, навіть за наявності скомпрометованого ключа власника інформації, зловмисник не отримає доступу до даних.

У загальному вигляді даний алгоритм представлений на рис. 4.

На першому етапі користувач вибирає файл на зовнішньому носії, над котрим необхідно виконати криптографічні перетворення.

Користувач вводить пароль, що буде використовуватись як перша частина ключа для шифрування відкритого тексту.

На другому етапі система зчитує серійний номер пристрою, на якому буде збережено файл і формує остаточний ключ для здійснення криптографічного перетворення. Отже, маємо ключ, сформований не тільки користувачем, який знає відкритий ключ, але й носієм, на якому воно зберігається. Надалі цей ключ можна адаптувати для обраного алгоритму шифрування, та перезаписати відкритий текст файлу на закритий.

Алгоритм передбачає зберігання таких файлів не тільки на знімних носіях типу USB FlashDrive, але і на всіх інших пристроях від зовнішніх жорстких дисків до мобільних телефонів.

Таким чином, отримуємо систему, яка дозволить зберегти інформацію, у разі викраденя її з носія даних, навіть при компрометації ключа користувача.

Висновки

Авторами було розроблено програмний продукт, що дає змогу зберегти важливу інформацію на робочих станціях від несанкціонованого копіювання самими користувачами. У ситуації коли користувач помилково, залишив ввімкнений комп'ютер, а потенційний зловмисник намагатиметься скопіювати важливі дані, програма також не дозволить йому це зробити.

Алгоритм захисту даних на зовнішніх носіях дає змогу шифрувати інформацію з використанням ідентифікатора середовища її зберігання. Таким чином, якщо шифрований текст буде скопійовано з носія, і ключ користувача буде скомпрометовано, то можна бути впевненими, що інформація розкрита не буде.

Таким чином, використання даного програмного продукту доцільне для захисту інформації в автоматизованих системах від витоку через знімні накопичувачі даних.

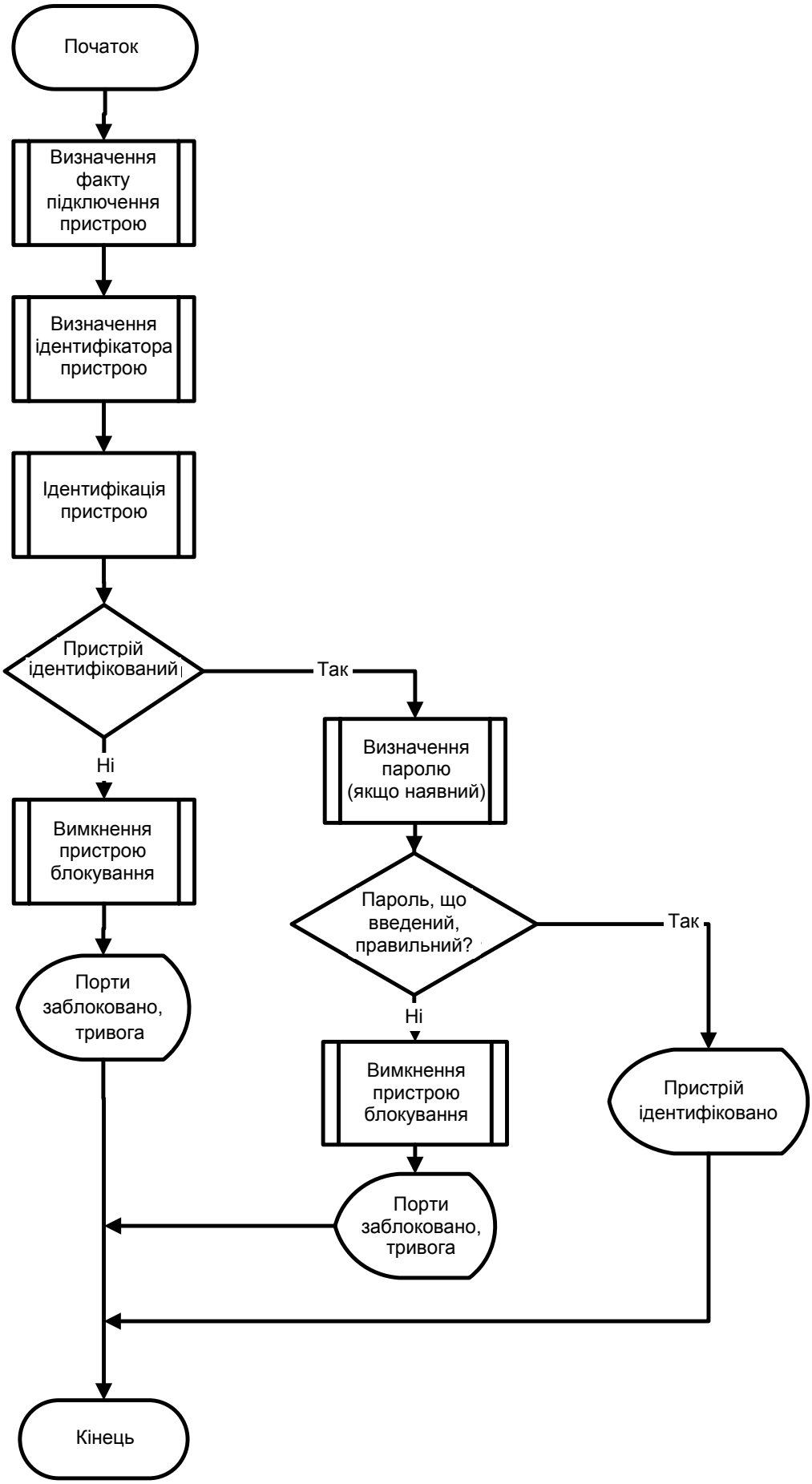

Рис. 3. Алгоритм здійснення моніторингу портів та перевірки пристроїв

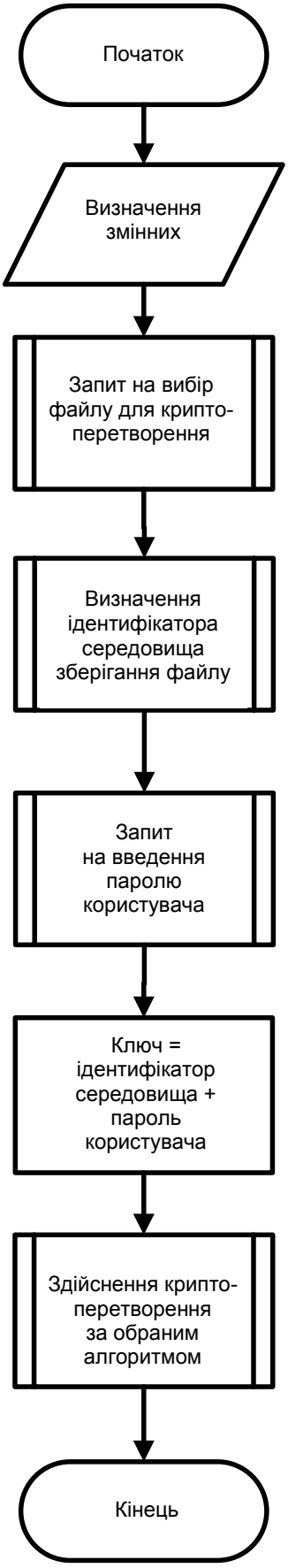

Рис. 4. Алгоритм прив’язки закритого тексту до середовища зберігання

ЛІТЕРАТУРА

1. *Варлатай С.* Программно-аппаратная защита информации: учеб. пособие/ С. Варлатай, М. Шаханов. — Владивосток : ДВГТУ, 2007.

2. *Карасик И. Г.* Программные и аппаратные средства защиты информации для персональных компьютеров / И. Г. Карасик // Компьютер-пресс, 1992, №3. — С. 37—46.

3. *Михайлов С. Ф.* Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах. Основные концепции: учеб. пособие / С. Ф. Михайлов, В. А. Петров, Ю. А. Тимофеев. — М .: МИФИ, 1995. — 182 с.

4. *Скиба В. Ю.* Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. — СПб. : Питер, 2008. — 320 с.

5. *Смирнов Ю. Б.* Секреты флэшек и винчестеров USB / Ю. Б. Смирнов. — БХВ-Петербург, 2009. — 438 с.

6. *Петренко А. Б.* Протидія витоку інформації через з'ємні носії в автоматизованих системах / А. Б. Петренко, Е. В. Бєтанов // Інформатика і комп'ютерні технології:VII міжнародна наук.-техн. конф.: зб. праць. — Донецьк : ДонНТУ, 2011. — С. 259—260.

7. *Петренко А. Б.* Дослідження вразливих місць систем захисту інформації при використанні e-Token / А. Б. Петренко, Є. В. Бєтанов // Защита информации: сб. науч. трудов. — К. : НАУ. — 2010. — Вып. 17. — С. 221—226.

8. *Петренко А. Б.* Електронні ключі в системі захисту інформації / А. Б. Петренко, Є. В. Бєтанов // Захист інформації з обмеженим доступом та автоматизація її обробки: наук.-техн. конф., зб. тез. — К. : НАУ, 2011. — С. 20—21.

9. *Петренко А. Б.* Обеспечение трехфакторной аутентификации / А. Б. Петренко, Е. В. Бєтанов // Безпека інформаційних технологій: наук.-техн. конф.: зб. тез. — К. : НАУ, 2011. — С. 68.

10. *Бетанов Е. В.* Противодействие потере информации через USB носители: зб. тез VIII Міжнародно-технічної конференції студентства та молоді «Світ інформації та телекомунікацій-2010». — Київ, 27-28 квітня 2011 р. — 77—78 с.

Стаття надійшла до редакції 17.05.2012.