УДК 004.056

В.Ю. КОРОЛЬОВ, В.В. ПОЛІНОВСЬКИЙ

КОНЦЕПЦІЯ ПОБУДОВИ ПЕРСОНАЛІЗОВАНИХ ФЛЕШ-НАКОПИЧУВАЧІВ ДАНИХ З АПАРАТНИМ ЗАХИСТОМ ІНФОРМАЦІЇ

Abstract: *The concept of building a personalized flash drives with a higher degree of security of confidential information is discussed. The solutions are based on Petri network models of processes of authentication of user and protection of portable data processing services.*
Key words: *information personalization, user authentication, security of portable services.*

Анотація: *Запропоновано концепцію побудови персоналізованих флеш-накопичувачів з підвищеним рівнем безпеки конфіденційної інформації. Розроблене рішення базується на моделях Петрі процесів автентифікації користувача і захисту портабельних сервісів обробки даних.*
Ключові слова: *персоналізація інформації, автентифікація користувачів, безпека портабельних сервісів.*

Аннотация: *Предложена концепция построения персонализированных флеш-накопителей с повышенной степенью безопасности конфиденциальной информации. Разработанное решение базируется на моделях Петри процессов аутентификации пользователя и защиты портабельных сервисов обработки данных.*
Ключевые слова: *персонализация информации, аутентификация пользователей, безопасность портабельных сервисов.*

1. Вступ

Сучасні флеш-накопичувачі інформації з USB-інтерфейсом утворюють клас масових мобільних пристроїв зберігання даних, що збільшують продуктивність праці користувачів персональних комп'ютерів (ПК).

Опитування, замовлене компанією SanDisk, показало, що 77% службовців використовують придбані ними флеш-накопичувачі як для особистих, так і пов'язаних з роботою задач. При цьому значна частина збережених даних відноситься до категорії конфіденційної інформації: записи про клієнтів (25%), фінансова інформація (17%), бізнес-плани (15%), контактна інформація службовців (13%), маркетингові плани (13%), інтелектуальна власність (6%), коди програм (6%).

Наведені дані доводять, що флеш-накопичувачі будуть доступними і затребуваними мобільними пристроями зберігання ділової і особистої інформації в найближчий період розвитку інформаційних систем.

2. Постановка задачі

Опитування виявило також, що можливість перенесення інформації з флеш-накопичувачів, обладнаних USB-інтерфейсом, представляє серйозну загрозу втрати і безпеки даних. Приблизно кожен десятий (12%) з користувачів корпоративних персональних комп'ютерів (ПК) повідомив, що йому доводилось знаходити флеш-накопичувач у місцях громадського користування. На питання про три найбільш імовірних дії, які службовці зробили б, якщо знайшли флеш-накопичувач у громадському місці, 55% відповіли, що продивились би усі дані.

Інше опитування, виконане у 2007 році компанією Fortune у Великобританії серед IT-професіоналів (IT – інформаційні технології), виявило, що дві третини IT-професіоналів, працюючих з мобільними накопичувачами, не використовують технології захисту збережених даних, не дивлячись на розуміння можливих загроз.

Тому актуальною науково-прикладною задачею є розробка персоналізованих флеш-накопичувачів (ПФН) з USB-інтерфейсом, якість захисту інформації яких мінімально залежить від людського фактора.

3. Технічні характеристики сучасних USB-флеш-накопичувачів

Техніко-економічні характеристики мобільних накопичувачів інформації з USB-інтерфейсом корпоративного класу з об'ємом пам'яті 4 ГБ та апаратно-програмним захистом інформації представлено у табл. 1.

Таблиця 1. Характеристики USB-флеш накопичувачів з апаратно-програмним захистом інформації [1]

№ n/n	Фірма-виробник	Вартість, дол. США	Швидкість читання|запису, МБ/с	Серверне ПЗ для КЖЦ* накопичувача
1	Kingston	191	24|10	–
2	SanDisk	144	24|20	CMC
3	IronKey	149	30|20	my.IronKey.com
4	Verbatim	130	30|12	mTrust
5	Kanguru	130	30|15	–
6	Imation	133	н/д	–
7	Mxisecurity	189	н/д	ACCESS Enterprise

*КЖЦ – керування життєвим циклом інформації.

Розглянуті корпоративні флеш-накопичувачі використовують автентифікацію користувача за допомогою вводу надійного пароля з клавіатури ПК з обмеженою кількістю спроб, пакети даних між флеш і ПК шифрують за алгоритмом AES-256, файли зберігають у закритій зоні пристрою. Зазначимо, що в наш час існує багато легкодоступних програм-шпигунів, що дозволяють отримати пароль, введений з клавіатури, причому за регламентом політик безпеки паролі змінюють не частіше одного разу на місяць. Якщо в середині мережі організації виконується облік використаного програмного забезпечення (ПЗ) і перевірка файлів, які приносять службовці, то поза межами корпорації гарантувати захист процесу вводу пароля практично неможливо. Тому при використанні флеш-накопичувачів за межами організації автентифікація користувачів за допомогою складних паролів не може гарантувати захист конфіденційної інформації від несанкціонованого доступу.

Вироби, що позиціонуються на ринку як професійні [1], підтримують також відкриту зону постійної пам'яті, розмір якої встановлюється у настройках мобільного пристрою зберігання. Таким чином, у випадку крадіжки, підміни або втрати накопичувача комерційно важлива інформація залишиться недоступною зловмисникам. Апаратно-програмне шифрування потоку даних між хост-комп'ютером і флеш-накопичувачем забезпечує суттєве збільшення захищеності конфіденційної інформації при роботі поза межами безпечної корпоративної мережі, в якій спеціалізовані програми контролюють потоки даних і порти. Тому не існує виключно високорівневих програмних рішень, які було сертифіковано FIPS, рівень 2 [1].

4. Технологія автентифікації користувачів з використанням ВІК-ключа

Автентифікація користувачів ПФН базується на використанні перестроюваного ключа-автентифікатора Бардаченка (ВІК-ключ) [2–5], який на сьогоднішній день містить 2^{14} варіантів кодової послідовності (рис. 1). У Центрі таймерних обчислювальних систем Інституту кібернетики виконуються науково-практичні розробки нового ключа автентифікатора, який матиме

Рис. 1. Зображення ВІК-ключа

не менше 2^{42}, а в подальшому планується довести цей показник до 2^{128}. І це все тільки механічним шляхом! Головною перевагою ВІК-ключа є оперативна зміна значень розрядів кодової комбінації вручну, тобто без будь-яких механічних або електронних допоміжних засобів. Крім того, ключ є стійким до електромагнітних і механічних впливів і не випромінює енергію. ВІК-ключ випускається серійно на ВАТ "Меридіан", і його вартість складає 0,4 дол. США. Таким чином, ВІК-ключ є одним із самих дешевих автентифікаторів.

ВІК-код – це стан ВІК-ключа, що визначається позиціями отворів на обертальних пластинах і їх положенням відносно осі, які представляють собою розряди двійкового числа. Отвори ВІК-ключа послідовно зчитуються рідером, який складається з двох оптопар і мікроконтролера (безконтактний спосіб вводу ключа [4, 5]).

Протягом останніх років у ЦТОС ІК було створено декілька алгоритмів обробки результатів безконтактного способу вводу ВІК-ключа для різних його конструкцій і типів мікроконтролерів [2–7].

Рекомендується послідовно вводити два 14-розрядних ВІК-ключа з різними ВІК-кодами, завдяки чому збільшується кількість кодових комбінацій і послаблюється вплив людського фактора [7]. Такий варіант введення кодової комбінації необхідний також для систем, що надають права доступу тільки при послідовному введенні двох ключів двома уповноваженими особами (принцип двох рук). У той же час кількість вводів ключа обмежується тільки зручністю експлуатації системи. Збільшення кількості розрядів введеного коду з 28 до криптографічного стандарту в 256 біт забезпечується алгоритмами розширення векторів коду [2] і регламентом ротації ключів [2].

Для авторизації доступу до обчислювальних ресурсів головною вимогою є стійкість системи до перебору ключів протягом заданого періоду часу, надійність і простота експлуатації, можливість оперативної зміни кодової комбінації ключа без використання зовнішніх засобів і їх низька вартість. Оперативність зміни кодової комбінації ключа дозволяє при його компрометації користувачу миттєво змінити старий ВІК-код на новий без необхідності заміни ідентифікатора або перепрошивання його носія. Крім того, оскільки автентифікатором є не сам ключ, а код, набраний на ньому, при необхідності існує можливість делегувати права доступу іншій особі при форс-мажорних обставинах. У свою чергу, оперативність зміни кодової комбінації дозволяє використовувати ключ у різних засобах безпеки, обладнаних рідерами ключа ВІК.

Ключ-автентифікатор Бардаченка є механічно перестроюваним, тому можливість комп'ютерного перебору 2^{28} кодових комбінацій при ідентифікації користувача виключається без зламу корпусу пристрою зчитування і доступу до його електричних кіл. Як правило, політикою безпеки кількість введень ключа обмежується п'ятьма спробами, після чого система блокується і видає сигнал тривоги. Тому доступ до терміналу шляхом механічного перебору є малоймовірним. Зазначимо, що кількість комбінацій для 4-значного десяткового PIN-коду банкоматів і мобільних телефонів, що мають фото/відео камеру, складає $10000 \approx 2^{13}$, у той час, як запропоноване рішення збільшує стійкість подібних систем до перебору у 2^{15} рази.

Крім того, при використанні ВІК-ключа для задач захисту інформації кількість розрядів ВІК-коду може бути збільшена за допомогою алгоритмів розширення вектора коду [2]. Таким чином, представлений спосіб авторизації користувача телекомунікаційних і обчислювальних засобів дозволяє досягти кращого співвідношення показників в області безпеки, ефективності експлуатації і вартості реалізації рішень, що підтверджено багатьма спеціалістами, у тому числі експертами Національного банку України (http://www.tau-systems.org.ua/news.php).

У даній роботі розглядаються два етапи автентифікації користувача при роботі з персоналізованими флеш-накопичувачами інформації. Перший етап автентифікації виконується вбудованим мікроконтролером у середині пристрою при підключенні флеш-накопичувачів інформації до USB-порту комп'ютера. Такий тип автентифікації автори називають імобілайзерним [6], оскільки пристрій не буде працювати при несанкціонованому включенні. На другому етапі у пристрій поступають дані, введені з клавіатури, а на виході з пристрою у високорівневу програму поступає складний пароль по захищеному протоколу обміну даними.

Таким чином, використання ВІК-ключа для автентифікації користувача флеш-накопичувача дозволяє захистити процес введення пароля від зчитування шпигунськими програмами при роботі на комп'ютері, який за звичайних обставин не контролюється корпоративною системою безпеки.

5. Принципи розробки персоналізованих пристроїв (ПП)

1) Безпека архітектури апаратно-програмних засобів – пристрій і програмне забезпечення повинні проектуватися так, щоб виконати автентифікацію власника ПП, забезпечити технічний захист своїх компонент від фізичного проникнення, тобто персоналізувати інформацію.

2) Захищеність комунікацій між хост-комп'ютером і ПП забезпечується протоколами захищених комунікацій і криптографічними алгоритмами.

3) Гарантія безпеки роботи з моменту першого використання ПП – вихідні установки апаратно-програмних засобів повинні забезпечувати захист конфіденційної інформації (мінімальний рівень привілеїв для роботи ПЗ, вимкнення рідко використовуваних сервісів і т.п.).

4) Підтримка користувачів – продукт супроводжується керівництвом користувача, на сайті виробника доступні оновлення ПЗ і функціонують сервісні служби для клієнтів.

Рис. 2. Структурна схема роботи ПФН

6. Концепція персоналізованого флеш-накопичувача

Структурна схема роботи ПФН, яка базується на перелічених принципах, наведена на рис. 2.

Зірочкою показано коло живлення контролера, завдяки якому і реалізована імобілайзерна автентифікація користувача. На рис. 3 показано функціональну схему роботи ПФН.

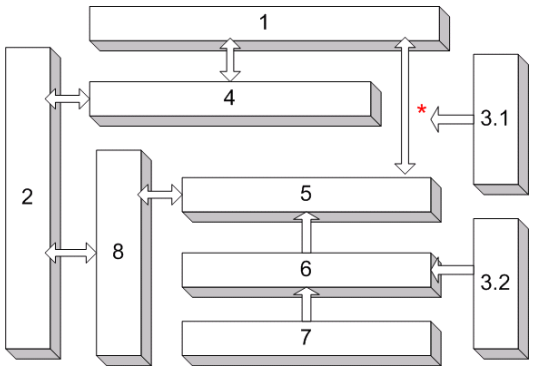

Рис. 3. Функціональна схема роботи утиліт ПФН

Розшифровка позначень:

1 – утиліта, що реалізує роботу з флеш-пам'яттю;

2 – утиліта, що реалізує роботу з USB-протоколом;

3.1 – утиліта персоналізації власника флеш-накопичувача;

3.2 – утиліта зчитування ключа;

4 – утиліта прямої (без шифрування) прийому/передачі даних;

5 – утиліта шифрування даних;

6 – утиліта генерування ключової послідовності;

7 – псевдогенератор;

8 – утиліта захисту комунікаційних протоколів (ПЗПІ – протокол з підвищеним захистом переданої інформації).

При підключенні персоналізованого флеш-накопичувача до USB-порту ПК на електричні кола контролера подається живлення і пристрій переходить у режим очікування вводу ключа у рідер. Далі виконуються два етапи автентифікації користувача:

I. Напівавтономний режим. Автентифікація користувача ПФН виконується за допомогою утиліт контролера (рис. 3). Після під'єднання ПФН до USB-порту на пристрій з ПК через вхід 2 подається живлення і активується режим очікування (запускаються мікропрограми зчитування ключа – 3.2 і персоналізації власника флеш-накопичувача – 3.1) вводу ВІК-ключа у рідер. При цьому необхідно зазначити, що всі інші кола живлення роз'єднані, тобто у даному режимі функціонує тільки рідер ВІК (рис. 2). При затіненні оптопар рідера починається процес зчитування ВІК-ключа. Кодова послідовність, зчитана з ключа-автентифікатора, передається в 3.1 для проведення процедури автентифікації. Якщо ключ вірний, то замикаються електричні кола ПФН і запускається другий етап автентифікації користувача. У випадку п'яти послідовних невірних спроб вводу ключа пристрій блокується, що дозволяє говорити про достатню захищеність ПФН від несанкціонованого доступу, навіть на цьому етапі [3, 7].

II. Підлеглий режим. Автентифікація користувача ПФН з використанням ресурсів ПК і утиліт мікроконтролера. Після успішної автентифікації користувача на першому етапі з відкритої частини флеш-пам'яті ПФН запускаються драйвери для ОС Windows для ПК і високорівнева програма "Персоналізація" з графічним інтерфейсом (рис. 3). Захищений обмін даними між мікропрограмами ПФН і високорівневими програмами ПК забезпечується ПЗПІ-протоколом – 8. Утиліта генерування криптостійких псевдовипадкових чисел – 6 використовує дані з псевдогенератора – 7, який використовує дані моніторингу станів мікроконтролера і параметри доступу до флеш-пам'яті від 1, крім того, на ці дані накладається послідовність з 3.2. Автентифікація завершується запуском меню оболонки портабельного ПЗ "ВІК-Сервіси", що містить набір необхідних оператору утиліт, з відкритої частини пам'яті – 1а. В результаті автентифікації користувач отримує доступ до закритої частини флеш-пам'яті – 1б, де зберігаються конфіденційні файли і документи у зашифрованому вигляді.

Після першого етапу автентифікації користувача контролер ПФН звертається до контролера USB-шини, ініціюючи пошук нових пристроїв диспетчером PnP-пристроїв ОС Windows.

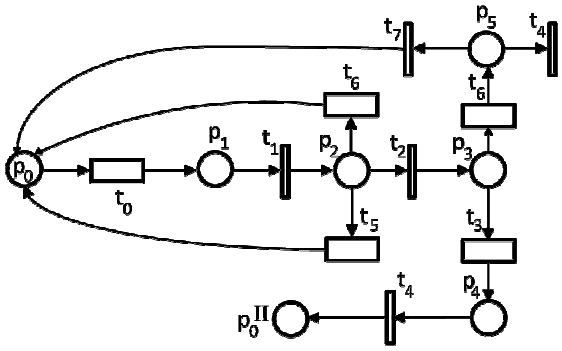

Рис. 4. Мережа Петрі для першого етапу автентифікації користувача ПФН (напівавтономний режим роботи)

7. Формалізація процесів автентифікації користувачів

Щоб формалізувати процес автентифікації користувачів ПФН, використаємо модель опису процесів за допомогою мереж Петрі [8]. Представлення системи мережею Петрі ґрунтується на двох поняттях: подіях і умовах. Події – це дії, що мають місце у системі. Виникнення подій керує станом системи. Стан системи може бути описано множиною умов. Умови представляють собою логічний опис системи до і після виконання подій. Для того, щоб подія сталася, необхідне виконання відповідних умов (передумов). Виникнення подій призводить до виконання інших умов (передумов). Виконання подій призводить до виникнення інших умов (наслідків). У мережах Петрі умови моделюються позиціями, події – переходами.

На рис. 4 та у табл. 2 представлено формальний опис процесу автентифікації користувачів у напівавтономному режимі роботи ПФН на базі мережі Петрі.

Таблиця 2. Напівавтономний режим роботи персоналізованого флеш-накопичувача (ПФН)

№ n/n	Передумови	Події	Наслідки
1	Вихідні умови [старт моніторингу вводу ключа, включено режим напівавтономної роботи] (p_0)	Введення ключа, включено блокування зчитування наступного ключа (t_0)	Введено ключ (p_1)
2	p_1	Перевірка помилок зчитування ключа (t_1)	Код зчитано вірно (p_2)
3	p_2	Верифікація хеш (t_2)	Хеш-сума вірна (p_3)
4	p_3	Старт головного контролера (t_3)	Флеш-накопичувач ініціалізовано (p_4)
5	p_4	Виконання початкових умов підлеглого режиму (t_4)	$p_{0\,\mathrm{II}}$
6	Ключ зчитано з помилками (p_2')	Розблокування повторного вводу ключів (t_5)	p_0
7	Хеш-сума невірна (p_3')	Обробка невірної комбінації, активовано лічильник спроб (t_6)	Дозволено повторне введення ключа (p_5)
8	p_5	Значення лічильника спроб зменшено на одиницю (t_7)	p_0
9	Повторне введення ключа не дозволено (p_5')	Вихід (t_4)	Немає

У табл. 3 та на рис. 5 представлено формальний опис процесу автентифікації користувачів у підлеглому режимі роботи ПФН на базі мережі Петрі.

Таблиця 3. Підлеглий режим роботи ПФН

№ n/n	Передумови	Події	Наслідки
1	Перший етап автентифікації пройшов успішно; дозволено перехід у підлеглий режим (p_0)	Запуск системних сервісів ОС Windows, відкриття порту, встановлення з'єднання по захищеному протоколу (t_0)	Диспетчер PnP пристроїв ОС Windows знайшов та ідентифікував новий пристрій (p_1)
2	p_1	Запуск програми START з ПФН. Очікування вводу автентифікаційних даних у меню програми імобілайзерного захисту (t_1)	Поля форми заповнені коректно, дозволено введення ключів у рідер (p_2)
3	p_2	Виклик мікропрограми зчитування ключа і передача хеш-суми пароля у ПФН (t_2)	Хеш-сума ключа і пароля перевірені (p_3)
4	p_3	Доступ до файлів ПФН (t_3)	Запуск меню пПЗ і виклик додатків (p_4)
5	p_4	Безпечне від відключення ПФН (t_4)	Завершення роботи (p_5)
6	p_5	Вихід (t_5)	Немає
7	p_1	Системна помилка (t_6)	Повернення у напівавтономний режим роботи (p_I)
8	p_3	Обробка невірного вводу ключа і пароля (t_7)	Зменшення лічильника спроб (p_7)
9	p_7	Запит оператору на повторне введення ключа (t_8)	p_2
10	p_7	t_5	Немає

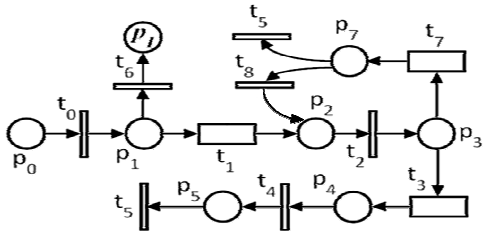

Рис. 5. Мережа Петрі для другого етапу автентифікації користувача ПФН (підлеглий режим роботи)

Обмін даними між ПФН і ПК під час роботи оператора з програмами оболонки "ВІК-Сервіси", як і другий етап автентифікації користувача, базується на ПЗПІ-протоколі, а всі тимчасові службові файли зберігаються на відкритій частині флеш.

8. Клієнт-серверний протокол з підвищеним захистом переданої інформації (ПЗПІ)

Протокол ПЗПІ відноситься до рівня додатків у семирівневій моделі OSI.

Структуру ПЗПІ-пакета показано на рис. 6.

Узагальнений алгоритм ПЗПІ-протоколу (без урахування особливостей технічної реалізації) передбачає виконання таких кроків:

1. Клієнт відправляє серверу свій ідентифікатор – несекретне число, що відповідає персоналізованому пристрою у базі даних серверу.

2. Сервер знаходить ідентифікатор клієнта у базі даних і зчитує секретний код клієнта. Якщо ідентифікатор відсутній у базі даних серверу, то обробка запиту переривається.

Адреса
Ключі обміну даними (Auth)
Хеш-сума даних
Розмір пакету
Поле даних або команд

Рис. 6. Структура пакета ПЗПІ

3. Сервер генерує сесійний ключ. Сесійний ключ (KS) – секретний код, який генерує сервер і використовує його протягом усіх трансакцій замість клієнтського секретного коду (SCk).

4. Сервер генерує ініціальний трансакційний ключ (KT_0). Трансакційний ключ — секретний ключ, що генерується сервером для кожного пакета даних (трансакції). Ініціальний трансакційний ключ розраховується сервером як хеш-функція від секретного коду клієнта: $KT_0 = hesh(SCk)$.

5. Сервер виконує операцію "Виключне АБО" (XOR) над сесійним і трансакційними ключами і відправляє результат у пакеті даних клієнту (поле ключі обміну даними).

$$Auth = KT_0 \otimes KS = XOR(KT_0, KS).$$

6. KT_0 розраховується клієнтом. Клієнт виймає сесійний ключ з пакета, відправленого сервером:

$$KS = XOR(Auth, KT_0).$$

7. Клієнт відправляє серверу пакет з командою-підтримкою отримання ключа.

8. Сервер генерує новий трансакційний ключ (KT_i), виконує операцію XOR з KT_0, а потім XOR з сесійним ключем:

$$Auth = XOR(KT_i, KS).$$

Результат вміщується у відповідне поле пакета.

9. Пакет даних шифрується новим трансакційним ключем і відправляється клієнту.

10. Клієнт виймає новий трансакційний ключ, шифрує їм пакет даних і відправляє його серверу.

Далі процес захищених комунікацій у відповідності з ПЗПІ-протоколом передбачає повторення кроків 4–10 при відправці кожного нового пакета.

9. Принципи проектування персоналізованих пристроїв

Розширити можливості зовнішнього оператора на ізольованому робочому місці дозволяє портабельне програмне забезпечення (Portable Software, пПЗ). Концепція пПЗ передбачає швидке розгортання на довільному ПК середовища з індивідуально налаштованим графічним інтерфейсом і значеннями опцій меню без повного перезавантаження операційної системи (ОС) робочого місця. Причому, основними апаратними засобами, для яких розробляється пПЗ, є USB-флеш-накопичувачі інформації.

Основною відмінністю портабельного ПЗ від стандартної Windows-програми є незалежність роботи додатку від версії і конфігурації Windows ОС і збереження налаштувань користувача після завершення сеансу роботи на ПК оператора – власника флеш-накопичувача.

Сучасні великі проекти в області обробки інформації базуються на принципах розробки надійного (trustworthy) ПЗ, які сформульовані фірмою Майкрософт у 2002 році (SD^3 + C парадигма:

Secure by Design, Secure by Default, Secure in Deploying, Communications), – безпека системи за побудовою, безпека настройок ПЗ за замовчуванням, безпечне впровадження, підтримка клієнтів). Нижче сформульовано принципи, які є розвитком цієї концепції. Вони були використані при проектуванні персоналізованих пристроїв (ПП) і портабельного ПЗ (пПЗ).

Опишемо процеси обробки електронних документів (файлів) з використанням персоналізованого накопичувача на флеш у вигляді мереж Петрі (табл. 4 та рис. 7).

Таблиця 4. Модель "Події-умови" для обробки файла

№ n/n	Передумови	Події	Наслідки
1	Встановлено захищене з'єднання між ПФН і ПК (p_0)	Виклик програми з оболонки пПЗ (t_0)	Програму відкрито (p_1)
2	p_1	Вибір файла з ПФН або хост-ПК (t_1)	Файл доступний (p_2)
3	p_2	Обробка файла: завантаження, редагування, відправка електронною поштою [Звернення до утиліт для отримання ключової послідовності для авторизації доступу до мережевих ресурсів, шифрування інформації і т.п.] (t_2)	Завершити редагування (p_3), p_1
4	p_3	Видалення тимчасових файлів і перехід у режим очікування (t_3)	p_0
5	p_3'	Видалити тимчасові файли (t_4)	p_1

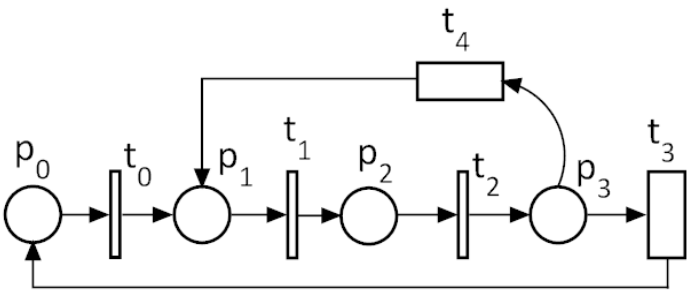

Рис. 7. Граф мережі Петрі для обробки файла

Рис. 8. Фотографія дослідного зразка ПФН

На рис. 8 представлено фотографію дослідного зразка ПФН, зробленого на українських підприємствах.

10. Висновки

1) Сформульовано принципи побудови мобільних накопичувачів даних з апаратною персоналізацією інформації і роботи портабельного програмного забезпечення.

2) Запропоновано формалізацію двофакторної автентифікації користувачів на базі моделі "події-наслідки" і графів мереж Петрі. Виконано аналіз стійкості роботи мереж Петрі і візуальне моделювання їх функціонування за допомогою програм емуляторів.

3) Представлено новий захищений протокол обміну даними між USB-флеш-накопичувачем і хост-комп'ютером.

4) Наведено мережу Петрі як приклад роботи портабельної програми обробки файлів на базі захищеного протоколу обміну даними.

СПИСОК ЛІТЕРАТУРИ

1. Королёв В.Ю. Обзор персонализированных флеш-накопителей корпоративного класса. http://www.tau-systems.org.ua/d/papers/o6z0pB.pdf.
2. Бардаченко В.Ф., Корольов В.Ю. Концепция построения систем персонализации на базе расширения вектора кодов ВІК-ключа // УСиМ. – 2007. – № 1. – С. 53 – 61.
3. Анализ современных средств аутентификации для систем защиты информации / В.Ф. Бардаченко, А.В. Кариман, О.К. Колесницкий и др. // УСиМ. – 2004. – № 3. – С. 81 – 92.
4. Персонализация мобильных телекоммуникационных и вычислительных средств методом оптической регистрации ВІК-кода / В.Ф. Бардаченко, В.Ю. Королёв, В.В. Полиновский и др. // УСиМ. – 2008. – № 2. – С. 46 – 53.
5. Королёв В.Ю. Алгоритмизация дистанционного распознавания ВІК-кода // Электронное моделирование. – 2008. – № 2. – С. 19 – 28.
6. Корольов В.Ю., Поліновський В.В., Малікова О.В. Побудова системи захисту інформації на базі персоналізованого USB-флеш з використанням ключа-ідентифікатора // Вісник Хмельницького національного університету. – 2008. – № 3. – С. 175 – 181.
7. Бардаченко В.Ф., Поліновський В.В., Костенко О.В. Побудова політики безпеки для інформаційних систем з використанням ВІК-ВАК технологій // Вісті академії інженерних наук України. – 2007. – № 1 (31). – С. 3 – 15.
8. Метод синтеза услуг в задачах компьютерной телефонии / А.В. Палагин, Н.И. Алишов, В.В. Полиновский и др. // Математичні машини і системи. – 2004. – № 3. – С. 89 – 101.

Стаття надійшла до редакції 10.12.2008