УДК 001.6+004

І.О. Громико, Д.Д. Тіллоєв

Харківський національний університет імені В.Н. Каразіна, Харків

ФЛЕШ-НОСІЇ З АКТИВНИМ ЗАХИСТОМ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Наданий варіант апаратурної реалізації стратегії і тактики активного захисту матеріальних носіїв інформації з обмеженим доступом. Автори сконцентрували свої зусилля на захисті ІзОД на флеш-носіях приватних осіб VIP-класу, які виконують спеціальні завдання банківських структур, воєнізованих організацій, армійських штабів і урядів. За основу автори взяли твердження про те, що скремблювання (скремблирование,-рос.) та будь-які криптографічні та стеганографічні методи захисту ІзОД можуть бути миттєво виявлені і дешифровані злочинцем.Виготовлений зразок захищеного флеш-носія показав комерційну ефективність і доцільність даного напрямку та заслуговує розвитку з допомогою фінансової підтримки досліджень державними і банківськими структурами.

Ключові слова: *флеш-носії, захист інформації, стратегія захисту інформації, тактика захисту інформації.*

Вступ

У суспільстві користувачів технічних засобів прийому, обробки, передачі та зберігання інформації (ТЗПІ) все ще превалює правовий інфантилізм, що виражається в неприпустимо толерантному підході до поведінки програмістів - авторів таких загроз, щодо інформації, як порушення її конфіденційності, цілісності, доступності та ін.

Втім, і в рядах наукової еліти СНД довго, а подекуди і сьогодні, існує благодушне ставлення до «витівок» відмінників навчання програмістів - студентів старших курсів, випускників вищих навчальних закладів. Навіть в 16-му розділі Кримінального кодексу України спочатку спостерігався різкий контраст між скоєним злочином і покаранням за комп‘ютерні злочини [1]. У фільмах, котрі приваблюють патріотичну молодь захоплюючими фантастичними сюжетами, хакерам відведена роль героїв, що рятують не тільки людей, які потрапили в складні життєві ситуації, але й все людство. Це і фільм «Армагеддон» (англ. – Armageddon), в якому хакер порушує супутниковий зв'язок рятуючи життя на Землі; і фільм Термінатор (англ. – TheTerminator), де хакер розкриває сейф з фатальним чіпом; і «День незалежності» (англ. – Independence Day) з порятунком людства шляхом хакерського зараження комп'ютерним вірусом ТЗПІ ворожої іноземної цивілізації; і Брат-2 – в якому за допомогою хакерського несанкціонованого доступу (НСД) до конфіденційної інформації вдається дізнатися координат злочинців; і так далі і тому подібне.

З 90-х років минулого століття по сьогоднішній день засобами масової інформації в дилетантському суспільстві сформована думка про суттєву віддаленість громадянського мирного життя від пригод з використанням комп'ютерної техніки. Відомий навіть випадок, коли на захисті дипломного проекту керівнику зроблено зауваження про недоречність застосування термінів «стратегія» і «тактика» в боротьбі з несанкціонованим доступом до конфіденційної інформації (ІзОД) в зв'язку з тим, що ця термінологія несе в собі агресивний характер і може бути застосованою лише в військових, армійських умовах.

Минуло небагато часу і людство дізналося про реалізовану на практиці програму Департаменту США «Чіпінг», про хакерські загрози і атаки на системи управління атомними електростанціями і міські енергосистеми. Зафіксовано і «недавній» випадок комп'ютерного шантажу шляхом здійснення хакерської атаки на системи життєзабезпечення медичного закладу та, навіть, управління роботою кардіостимуляторів.

Фінансові і політичні претензії хакерів, які поєднуються з впливом на роботу життєве важливих ТЗПІ, підвели людство до межі, за якою подальша добродушність і лицемірство неприпустимі.

Хакери оголосили людству війну.

І не важливо, добровільно, амбітно або під зовнішнім тиском відбуваються правопорушення, які можна класифікувати як злочин. Йдеться про інформаційні загрози, реалізація яких вже зараз неодноразово ставить людей на грань “життя/смерть”.

Агресивна відповідь на такі загрози доречна і безумовно необхідна.

«Агресивна відповідь на атаку» – таке судження чимось схоже на словосполучення «перевищення меж необхідної самооборони». Розглянемо приклад. Якщо, припускаємо існування злочинного пристрою (для підслуховування наших конфіденційних розмов в нашій корпоративній мережі) і з метою його зни-

щення ми подаємо в провідну лінію зв'язку високовольтний імпульс, то чи потрібно нам переживати про збитки, завдані правопорушнику? На перший погляд – ні. Однак … а якщо нас підслуховує «псевдо правопорушник», тобто юридична особа з численних рядів правоохоронних органів, який отримав на здійснення своїх дій санкцію прокуратури? Адже спалено державне майно – дорогоцінна апаратура контролю та розвідки. І неважливо, корумпована чи ні та фізична особа, що діє під парасолькою статусу юридичної особи. Робітник цієї структури може (і, мабуть, зможе) знайти правове виправдання своїм діям, а ми отримаємо проблему у вигляді кадрових (на тлі масових звільнень в період кризи) та фінансових втрат. Це тільки одна з вагомих причин, що лежать в основі процвітання хакерського свавілля в країнах світу [2].

Крім того треба пам‘ятати про хронічне відставання засобів захисту від розвитку засобів інформаційної розвідки [3].

Автори цієї роботи пішли на компроміс, замінив словосполучення «агресивна відповідь на хакерську атаку» словом «активна» (дія), залишив, при цьому, «стратегію» та «тактику» в боротьбі проти злочинів у віртуальному кіберпросторі. Аналогічний військовий погляд на боротьбу з кіберзлочинством проглядається в планованих діях блоку НАТО та в державному підході, висвітленому у рішенні Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [4]. Екстремістські організації та злочинні структури не дивлячись на наслідки своїх дій та без будь-яких розмов про гуманність активно використовують інформаційні технології для реалізації своїх злочинних намірів. У такій ситуації є саме злочином міркування про гуманне ставлення до кіберзлочинців розмовляючи про «перевищення меж необхідної самооборони». Вже відбулася міжнародна конференція присвячена проблемам кіберзахисту «4rd InternationalConferenceonCyberConflict», де лейтмотивом лунала тема про можливість військової і воєнізованої відповіді на дії кіберзлочинців [5].

Сьогоднікіберпростір є ареною конфліктів між державами, організаціями та приватними особами [6]. Тому автори цієї роботи сконцентрували свої зусилля на захисті ІзОД, яка розміщена в флеш-носіях приватних осіб VIP-класу, які виконують спеціальні завдання банківських структур, воєнізованих організацій, армійських штабів і урядів.

Основна частина

На сьогоднішній день існує багато методів, засобів та пристроїв захисту інформації, як поширюються від джерела до отримувача завдяки наявності між ними ланцюжка носіїв інформації [2]. З одного боку ці ланцюжки є аналогом транспортних артерій і вельми корисні для реалізації інформаційних відносин. З другого боку, – кожному з них присутні параметри та характеристики, які позитивно або негативно впливають на якість інформаційного процесу прийому, передачі, обробки (та т. п.) інформації.

Ці параметри та характеристики можна корегувати або зовсім змінювати застосувавши інший носій, що дозволяє попередити потенційне правопорушення проти власника інформації. Зрозуміло, що служби захисту інформації в усіх країнах світу працюють «по-старинці» і не завжди сприймаючи до розуму вимоги попереджуючої стратегії захисту інформації [7]. Справа у тому, що за попереджуючою стратегією боротьби з кіберзлочинством повинна йти тактика, яка, в свою чергу, дозволяє розробити щаблини структурних та функціональних схем систем захисту, після чого прослідують схеми засобів захисту у вигляді приладів (пристроїв та ін.). А це вже задача, яка посильна тільки спеціалістам високого класу.

Огляд останніх досліджень та публікації

Тема допоміжних зовнішніх носіїв інформації актуальна і надзвичайно широка. Багато фахівців в області захисту інформації зосередили свою увагу на питаннях захисту інформації флеш-носіїв. Флеш-драйви, а в призначеному для користувача середовищі – флешки, стали причиною широкої популярності компактних засобів для зберігання та просторового поширення інформації. Їх масове використання спричинило посилення таких проблем, як втрата флеш-носія, крадіжка, несанкціоноване знімання інформації за допомогою портативних пристроїв - дублікаторів, знищення інформації та ін. [8].

Відповідно, розробники впровадили ряд методів по захисту інформації на флеш-носіях. До них належать різноманітні конструктивні та апаратно-програмні рішення.

Флешки і додаткові пристрої, що керують їх роботою, стали оснащувати радіопередавачами малої потужності для запобігання випадкам втрат інформації та для боротьби з НСД до ІзОД при значному видаленні флешки від її «господаря». Корпус флеш-драйвів стали виготовляти з міцних матеріалів, доповнюючи захист роз'ємів USB 2.0 звичайним механічним набірним замком. Додаткова клавіатура на корпусі дозволила впровадити в процес допуску локальний парольний захист.

На корпусах встановлюють потайливі кнопки, натискання яких може призвести до блокування інформації або її повного знищення. Почали широко застосовувати шифрування ІзОД, що знаходиться на флеш-носії.

Шифрувальні утиліти використовують 128-бітове шифрування AES, яке практично неможливо

зламати різними хакерськими «примочками», наприклад, використовуючи PasswordRemover [8 – 10].

Використовується також алгоритм шифрування AES з ключем 256 bit, схвалений NIST. З допомогою різних програмних продуктів типу RohMinDriv створюють на флеш-пам'яті зашифровані ділянки віртуального диску, де розміщують зашифровану секретну інформацію. Шляхом реалізації апаратно-програмних методів, флешки комплектують спеціальними пристроями які позволяють повністю знищити інформацію, якщо буде здійснена спроба несанкціонованого доступу до ІзОД. Флешки стали доповнювати сканерами, які допускають за папілярним узором на пальці різних користувачів до тієї чи іншої інформації [11 – 13].

Флешки все більш за своїми якісними показниками в користуванні стають схожими на банківські платіжні пластикові картки. При цьому слід вказати на те, що захисні (проти НСД) засоби стеганографії та криптографії, якими складними вони б не були, завжди розшифровуються кіберзлочинцями.

Можна перерахувати безліч методів і пристроїв захисту флеш-пам'яті від НСД і проти порушення цілісності інформації. Однак, враховуючи їх застарілу основу, розглянемо реально працюючий варіант захисту інформації, що здійснюється шляхом упереджування можливих дій правопорушника у відношенні до інформації на флеш-носії, зовнішній вигляд котрого та електричні параметри і характеристики не відрізняються від широко поширеного флеш-носія, що знаходиться у відкритому продажі.

Стратегія захисту флеш-драйву від НСД

Користувачі, які працюють з ІзОД, добре знають, що розголошення деяких відомостей, що є таємницею, може завдати шкоди національній безпеці України [14]. Тому не припустимо майже одноразовий витік інформації.

При роботі з ІзОД не можна бездіяльно очікувати сучасних розробок майбутніх методів захисту інформації майже при наявності загрози реального злочинства з застосуванням діючих методів порушення конфіденційності інформації.

Несанкціонований доступ до інформації з обмеженим доступом, яка зберігається на флеш-носіях, може здійснюватися особою, що переслідує досягнення цілей, що не збігаються з думкою і бізнес-планами власника інформації. В іншому випадку власником інформації було б санкціоноване для цієї особи право законного отримання даної інформації.

Ще у 1992 році Законом України «Про інформацію» було встановлено, що підстава для набуття права власності на інформацію виникає у випадках [15, ст.38]:

– створення інформації своїми силами і за свій рахунок;

– наявності договору на створення інформації;

– наявності договору, що містить умови переходу права власності на інформацію до іншої особи.

Таким чином, нехтування правом власності (правопорушення), на інформацію, наприклад, - НСД, тягне за собою нанесення матеріальної шкоди власнику інформації у вигляді: некомпенсованих витрат на створення інформації, втрати передбачуваного прибутку, пільг і т. д.

З викладеного вище слідує, що з точки зору власника ІзОД доцільне справедливе користування трьома базовими принципами, які становлять фундаментальну основу стратегії активного захисту та мають право на втілення у теорію та практику забезпечення інформаційної безпеки:

1. У разі здійснення атаки на інформацію, та засоби її захисту, припустимо нанесення адекватного матеріального збитку по відношенню до злочинного майна правопорушника. Наприклад, виведення з ладу знарядь правопорушення (у деяких випадках, – знарядь злочину): предметів, пристроїв, приладів, програм (тощо) з допомогою яких здійснювалося чи був вчинений злочин.

2. Власнику інформації, в процесі протидії спробам НСД не завжди потрібно строго обов‘язково обмежуватися межами будь-яких стандартів, настанов, правил та інструкцій. Стаття 41 Конституції України однозначно стверджує: «Ніхто не може бути протиправно позбавлений права власності. Право приватної власності є непорушним».

3. Дії по захисту інформації зобов'язані бути випереджальними.

Тактика боротьби з НСД до інформації на флеш-носіях

Для реалізації елементів вищезазначеної стратегії необхідно дотримання наступних умов:

1. Функціональні елементи активних (агресивних) ключів управління та захисту (АКУЗ) повинні бути недоступні правопорушнику і розташовуватися всередині самої конструкції ключа, тобто між комп'ютером і флеш-носієм.

2. АКУЗи повинні бути узгоджені з адаптованими (в ракурсі їх активності і агресивності по відношенню до техніки правопорушника) флеш-носіями і володіти наступним набором функцій:

– робити неможливим застосування будь-якого іншого неадаптованого флеш-носія спільно з АКУЗ;

– відкривати комп'ютеру доступ до інформації, яка розміщена на флеш-носії;

– періодично виводити з ладу підключені до АКУЗ флеш-носії правопорушника або його спеціальну апаратуру, яка застосовується для виявлення режимів функціонування елементів захисту інформації.

3. Адаптованість флеш-носія власника інформації передбачає наявність в його конструкції еле-

ментів і програм, які нейтралізують активні (агресивні) параметри АКУЗ, що призводять до руйнування флеш-носії правопорушника або його спеціальної апаратури. За всіма параметрами і характеристиками адаптований флеш-носій власника інформації повинен бути ідентичний неадаптованому в межах похибки вимірювання напруги, струмів та ін. При цьому, енергоспоживання адаптованого до АКУЗ флеш-носія не повинно відрізнятися від енергоспоживання неадаптованого флеш-носія в межах розкиду параметрів і характеристик радіоелементів, а також величини похибки вимірювання цих параметрів.

Приклад реалізації стратегії і тактики реалізується функціональною схемою – флеш-носія з ключем захисту від НСД (рис. 1).

Апаратурна реалізація приведена на рис. 2. Тестування та апробація показала високу надійність та стійкість до впливу програм та приладів на флеш-драйв з метою НСД до флеш-носія з ІзОД.

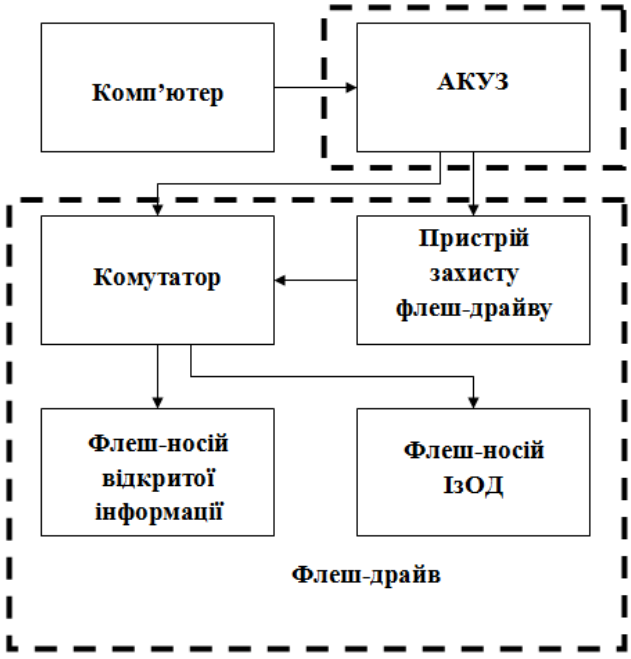

Рис. 1. Функціональна схема, що реалізує
базові принципи тактики активного захисту флеш-носіїв

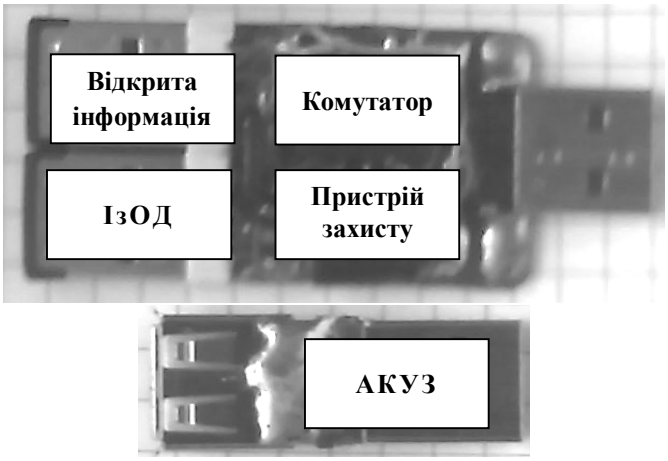

Рис. 2. Апаратурна реалізація функціональної схеми

Висновки

1. Упереджувальна активна стратегія захисту інформації на флеш-носіях від НСД є одним з перспективних напрямків захисту інформації, що створює правопорушникам наступні труднощі в здійсненні несанкціонованого доступу:

– необхідність попереднього дослідження АКУЗ перед здійсненням несанкціонованого доступу до ІзОД;

– необхідність захисту дослідницької або розвідувальної апаратури від апріорі невідомих факторів АКУЗ, які знищують вхідні елементи цієї апаратури;

– необхідність подолання інших моментів (шифрування, паролі, замки та ін.), приведених раніше.

2. Апаратурна реалізація активної стратегії показала її дієвість у процесі протидії НСД.

3. Виготовлений зразок захищеного флеш-носія показав комерційну ефективність і доцільність даного напрямку та заслуговує подальшого розвитку за допомогою фінансової підтримки досліджень державними і банківськими структурами.

Список літератури

1. Громыко И.А. К определению вида и размера наказания за компьютерные преступления в соответствии с Уголовным кодексом Украины / И.А. Громыко, Н.Ф. Логвиненко, В.В. Носов, П.И. Орлов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – Вип. 3. – С. 45-50.

2. Громыко И.А. Общая парадигма защиты информации: монография / И.А. Громыко. – Х.: ХНУ имени В.Н. Каразина, 2014. – 216 с.

3. Громыко И.А. Будущее за упреждающими системами защиты / И.А. Громыко, С.Ю. Кильмаев, Е.Я. Оспищев // Защита информации. INSIDE. – 2007. – С. 14-18.

4. Стратегія кібербезпеки України. Указ Президента України № 96/2016 від 15 березня 2016 року. м. Київ. - [Електронний ресурс] – Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/96/2016.

5. Марков В.В. Напрями діяльності НАТО у справі протидії кіберзлочинності / В.В. Марков, О.В. Караченцев // Право і безпека. – 2014. – № 4 (55). – С. 119-123.

6. Котух Є. Кіберзброя: проблеми та перспективи протидії кіберзлочинності: 24 квіт. 2012 р. [Електронний ресурс] / Євгеній Котух // З.С.: зовнішні справи : [сайт] / UA ForeignAffairs. – Режим доступу до сайту: http://www.uaforeignaffairs.com/en/expert-opinion/view/article/kiberzbroja-problemi-ta-perspektivi-protidiji-kiberzlo/.

7. Громико І.О. Випереджаюча активна стратегія захисту інформації з прикладом реалізації на флеш-носіях / І.О. Громико // Системи управління, навігації та зв'язку. – Полтава: ПНТУ ім. Ю.Кондратюка, 2013. – Вип. 2 (26). – С. 101-104.

8. Как защитить компьютер от несанкционированного доступа с помощью флэшки? [Електронний ресурс]. – Режим доступу до ресурсу: http://speak-pro-software.ru/wiki.

9. Как защитить паролем usb-накопитель. [Електронний ресурс]. – Режим доступу до ресурсу: http://data-repair.ru/theory/flash-drive-theory/kak-zashhitit-parolem-usb-nakopitel-ili-vneshniy-zhestkiy-disk.html.

10. Программа для установки паролей на локальные папки и флешки. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.addnew.com.ua/softsystem/news84.html.

11. Вопросы и ответы по защите информации. [Електронний ресурс]. – Режим доступу до ресурсу: http://otvet.mail.ru/question/54420302.

12. Букин М.И. Защита флэшек. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.pcweek.ru/mobile/article/detail.php?ID=115551.

13. Как защитить информацию на флэшке. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.pccare2.ru/content/view/3/.

14. Закон України «Про державну таємницю» Відомості Верховної Ради України (ВВР), 1994. – N 16. – ст. 93.

15. Закон України "Про інформацію». Відомості Верховної Ради України. – 1992. – N 48.

Надійшла до редколегії 11.05.2016

Рецензент: д-р екон. наук, доц. С.В. Кавун, Харківський учбово-науковий інститут банківської справи ДВНЗ «Університет банківської справи», Харків.

ФЛЕШ-НОСИТЕЛИ С АКТИВНОЙ ЗАЩИТОЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

И.А. Громико, Д.Д. Тиллоев

Представлен вариант аппаратурной реализации стратегии и тактики активной защиты материальных носителей информации с ограниченным доступом. Авторы сконцентрировали свои усилия на защите ИЗОД на носителях флеши частных лиц VIP-класса, которые выполняют специальные задания банковских структур, военизированных организаций, армейских штабов и правительств. За основу авторы взяли утверждение о том, что скремблирование и любые криптографические и стеганографические методы защиты ИЗОД могут быть мгновенно обнаружены и дешифрованы преступником.Изготовленный образец защищенного флеш-носителя показал коммерческую эффективность и целесообразность данного направления и заслуживает развития с помощью финансовой поддержки исследований государственными и банковскими структурами.

Ключевые слова: *флеш-носители, защита информации, стратегия защиты информации, тактика защиты информации.*

FLASH DRIVE WITH AN ACTIVE PROTECTION FROM UNAUTHORIZED ACCESS

I.A. Gromyko, D.D. Tilloiev

The article presents hardware implementation of the strategies and tactics for active protection of the physical storage media with a restricted access. The authors' efforts focus on the protection of information restricted in access (IRA) on flash drives of private VIPs who carry out specific tasks for banking institutions, paramilitary organizations, military headquarters and governments. The article is based on the assertion that scrambling as well as any other cryptographic and steganographic methods of IRA protection are subject to instant identification and decryption by the offenders. The produced sample of a protected flash drive proved the commercial efficiency and viability of this field, thus, further research deserves to be developed with the financial assistance of the state and banking institutions.

Keywords: *flash drive, information protection, information protection strategy, information protection tactics.*