

Я. О. Завацький, М. Г. Домненко, І. М. Колесникова

КОМПАКТНИЙ НОСІЙ ДАНИХ З ПРИХОВАНОЮ АПАРАТНОЮ АКТИВАЦІЄЮ ДЛЯ ОПЕРАТИВНОГО ВИКОРИСТАННЯ

Анотація. Розглянуто концепцію компактного носія даних з прихованою апаратною активацією для оперативного використання. Запропоновано підхід до модифікації USB-накопичувача шляхом інтеграції магнітокерованого комутаційного елемента, що дозволяє блокувати ініціалізацію пристрою без виконання визначеної фізичної умови активації. Така реалізація може бути використана для приховування факту працездатності носія, зниження ризику несанкціонованого доступу до інформації та підвищення рівня контролю доступу до даних у польових і службових умовах.

Ключові слова: компактний носій даних, прихована апаратна активація, USB-накопичувач, магнітокерований елемент, геркон, фізичний контроль доступу, захист інформації, оперативне використання.

Abstract. The paper considers the concept of a compact data storage device with concealed hardware activation for operational use. An approach is proposed for modifying a USB flash drive by integrating a magnetically controlled switching element, which makes it possible to block device initialization unless a specific physical activation condition is met. Such an implementation may be used to conceal the operational status of the storage device, reduce the risk of unauthorized access to information, and enhance the level of access control to data in field and service conditions.

Keywords: compact data storage device, concealed hardware activation, USB flash drive, magnetically controlled element, reed switch, physical access control, information protection, operational use.

Вступ

В умовах службової та оперативної діяльності, зокрема у сферах, пов'язаних із підвищеними вимогами до конфіденційності, особливого значення набуває захист цифрових носіїв інформації від несанкціонованого доступу та виявлення. Традиційні програмні засоби захисту не завжди забезпечують належний рівень маскування факту наявності працездатного носія, що створює потребу у впровадженні додаткових апаратних рішень [1].

Одним із перспективних підходів є використання компактного носія даних з прихованою апаратною активацією, принцип роботи якого передбачає блокування ініціалізації USB-накопичувача до моменту дії визначеного фізичного тригера. Такий підхід дозволяє підвищити рівень фізичного контролю доступу до інформації та розширити можливості безпечного використання носія в польових і службових умовах.

Результати дослідження

Компактні носії даних залишаються поширеним засобом перенесення та короткочасного зберігання інформації у службовій, оперативній і польовій діяльності. Водночас стандартні USB-накопичувачі мають суттєвий недолік: у разі підключення до пристрою вони автоматично ініціалізуються, що дозволяє сторонній особі одразу виявити працездатність носія та потенційну наявність на ньому даних. За умов підвищених вимог до конфіденційності це створює додаткові ризики несанкціонованого доступу, компрометації інформації та виявлення самого факту використання носія як засобу зберігання службових матеріалів.

У межах роботи розглянуто підхід до створення компактного носія даних з прихованою апаратною активацією, принцип якого ґрунтується на модифікації конструкції USB-накопичувача. Суть запропонованого рішення полягає у вбудуванні магнітокерованого комутаційного елемента в електричне коло між USB-роз'ємом і платою накопичувача. За відсутності магнітного впливу електричне коло залишається розімкненим або перебуває в неактивному стані, унаслідок чого накопичувач не проходить стандартну процедуру ініціалізації під час підключення. За наявності

визначеного фізичного тригера, реалізованого у вигляді магніта, розміщеного в ковпачку, відбувається замикання кола, що забезпечує працездатність пристрою та доступ до інформації.

Запропонована конструкція дозволяє реалізувати додатковий рівень фізичного контролю доступу без зміни стандартного зовнішнього інтерфейсу носія. Це забезпечує приховування факту працездатності пристрою для необізнаного користувача, оскільки в звичайному режимі підключення накопичувач не визначається операційною системою як активний USB-пристрій. Таким чином, досягається ефект апаратного маскування, за якого стороння особа може сприймати носій як несправний або неактивний.

Результати концептуального аналізу показують, що запропонований підхід має практичну цінність для службового та оперативного застосування, де важливими є компактність, простота використання, автономність та мінімізація демаскувальних ознак. На відміну від виключно програмних засобів захисту, апаратна активація не залежить від операційної системи, встановленого програмного забезпечення чи політик доступу на стороні хост-пристрою. Це розширює можливості використання модифікованого носія в умовах, де потрібен швидкий контрольований доступ до даних із мінімальним часом підготовки[2].

Окрему увагу приділено перспективі розширення базової конструкції. Зокрема, розглядається можливість створення дворежимного носія, у якому за відсутності магнітного впливу активується один режим роботи, а за його наявності – інший. Такий підхід теоретично дозволяє реалізувати не лише повне блокування ініціалізації, а й перемикання між різними режимами доступу до інформації. Наприклад, один режим може бути призначений для демонстрації нейтрального або допоміжного вмісту, тоді як інший – для доступу до основних даних. Подібне розширення підвищує гнучкість використання пристрою та рівень прихованості інформації.

Проведений аналіз також показує, що ефективність запропонованої конструкції залежить від низки технічних чинників, серед яких точність розміщення магнітокерованого елемента, стабільність його спрацювання, захищеність від випадкової активації та збереження механічної міцності корпусу після модифікації. Для практичної реалізації важливими є також мініатюризація компонентів, узгодження електричних параметрів схеми та забезпечення надійної роботи накопичувача після багаторазових циклів підключення[3].

Отже, запропонована концепція компактного носія даних з прихованою апаратною активацією може розглядатися як перспективний напрям удосконалення засобів фізичного захисту інформації. Її використання потенційно дозволяє знизити ризик несанкціонованого виявлення носія, ускладнити несанкціонований доступ до даних та підвищити рівень контролю над використанням цифрової інформації у службових, оперативних і польових умовах.

Висновки

У результаті проведеного дослідження встановлено, що концепція компактного носія даних з прихованою апаратною активацією може розглядатися як доцільний напрям удосконалення засобів фізичного контролю доступу до інформації. Використання магнітокерованого комутаційного елемента в конструкції USB-накопичувача забезпечує можливість блокування його ініціалізації за відсутності визначеного фізичного тригера, що підвищує прихованість пристрою та ускладнює його несанкціоноване використання. Подальший розвиток даної концепції доцільно пов'язувати з підвищенням конструктивної надійності, оптимізацією схемної реалізації та розширенням функціональності шляхом впровадження багаторежимного доступу до даних.

Список використаних джерел:

1. A novel mutual authentication scheme for USB storage devices. <https://dl.acm.org/doi/10.1145/1806338.1806413>.
2. Hardware-Based Methods for Electronic Device Protection against Invasive and Non-Invasive Attacks. <https://www.mdpi.com/2079-9292/12/21/4507>.
3. Best Practices for Removable Media Security. <https://www.opswat.com/blog/removable-media>.

***Завацький Ян Олександрович** – студент, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: omniameatecumporto1002@gmail.com.*

Домненко Микола Григорович – старший викладач кафедри військової підготовки, Вінницький національний технічний університет, м. Вінниця, e-mail: mikoladomnenko568@gmail.com.

Колесникова Інна Миколаївна – викладач Вінницький національний технічний університет, Вінниця, e-mail: innakolesnykova153@gmail.com

Zavatsky Yan Oleksandrovich – student of group 1SP-23b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: omniameamecumporto1002@gmail.com

Domnenko Mikola Grigorovich – speaker of the Department of Military Training, Vinnytsia National Technical University, Vinnytsya, e-mail: mikoladomnenko568@gmail.com.

Inna Mykolaivna Kolesnykova – Lecturer, Vinnytsia National Technical University, Vinnytsia, e-mail: innakolesnykova153@gmail.com