УДК 004.056

В. О. Кохановський
В. В. Гуменюк

УДОСКОНАЛЕННЯ ЗАХИСТУ PIN-КОДОВОГО ДОСТУПУ ВІД ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ЗАЛИШКОВІ ТЕПЛОВІ СЛІДИ НА КЛАВІАТУРНИХ ПАНЕЛЯХ

Вінницький національний технічний університет

Анотація

Об’єктом вивчення є інформаційні витоки, що виникають внаслідок залишкових теплових слідів на інтерфейсі введення цифр. У межах роботи розроблено нову математичну модель оцінювання захищеності, що базується на сукупності геометричних, часових та конструктивних параметрів. Проаналізовано чинники, які впливають на ризик зловмисного розкриття PIN-коду, зокрема кількість виявлених теплових відбитків, час їх згасання та тип клавіатурної панелі Практична цінність результатів полягає у визначенні ризику підходів, що дозволяють підвищити рівень конфіденційності PIN-кодів у сучасних системах контролю доступу.

Ключові слова: PIN-код, теплові відбитки, побічний канал витоку інформації, оцінювання ризику, захист інформації.

Abstract

The focus of this research is information leakage that may occur due to residual thermal traces left on a numeric keypad. During the study, a novel mathematical approach for evaluating security levels was proposed, which integrates geometric, temporal, and structural characteristics. The analysis considered several factors that influence the probability of unauthorized PIN code recovery, such as the quantity of observable thermal marks, the duration of their cooling process, and the specific keypad design. The practical significance of the obtained results lies in identifying methods for reducing such risks, thereby improving the protection and confidentiality of PIN codes in contemporary access control systems.

Keywords: PIN code, thermal attack, side channel, keypad panel, risk assessment, information security.

Вступ

PIN-кодовий доступ широко застосовується в банківських терміналах, електронних замках, системах контролю та управління доступом. Разом із традиційними загрозами несанкціонованого доступу дедалі більшого значення набувають побічні технічні канали витоку інформації. Одним із таких каналів є залишкові теплові сліди на поверхні клавіш після введення PIN-коду.

Актуальність дослідження зумовлена тим, що теплова інформація може бути отримана без втручання в програмне забезпечення або мережеву інфраструктуру, а отже потребує окремого врахування під час проєктування засобів захисту. Метою роботи є удосконалення оцінювання ризику витоку інформації через залишкові теплові сліди та формування рекомендацій щодо його зниження.

Результати дослідження

Аналіз літературних джерел показав, що в сучасних інформаційних системах необхідно враховувати не лише прямі загрози несанкціонованого доступу, а й можливі витоки інформації через побічні технічні канали [1]. Ефективність теплового спостереження залежить від матеріалу поверхні клавіш, температури навколишнього середовища, часу між введенням PIN-коду та моментом спостереження, а також від типу клавіатурної панелі. Зокрема, встановлено, що пластикові панелі мають низьку теплопровідність, що сприяє збереженню теплових слідів, тоді як металеві поверхні через високу теплопровідність забезпечують швидше розсіювання тепла [2]. Найвищий ризик характерний для статичних панелей із повільним тепловим згасанням, тоді як динамічне перемішування цифр істотно зменшує інформативність залишкових теплових слідів [3]. Відповідно до положень комплексного захисту інформації, викладених у [4], під час проєктування захищених систем необхідно враховувати сукупність можливих загроз і каналів витоку даних. У цьому контексті залишкові теплові сліди на клавіатурних панелях доцільно розглядати як фізичний побічний канал витоку інформації, що потребує окремого аналізу та врахування при оцінюванні захищеності PIN-кодового доступу.

Базовий підхід до оцінювання ризику можна подати як відношення кількості виявлених теплових слідів до довжини PIN-коду:

$$R_{base} = m / k,$$

Для підвищення точності оцінювання запропоновано удосконалену модель:

де R_{base}– базовий показник ризику; m – кількість виявлених теплових слідів; k – довжина PIN-коду. Такий підхід є простим, однак не враховує часову динаміку згасання теплових слідів, конструктивні особливості панелі та реальне зменшення простору пошуку PIN-комбінацій.

Для підвищення точності оцінювання запропоновано модель:

$$R_{th} = w_1 \cdot (m/k) + w_2 \cdot e\text{^}(-\lambda t) + w_3 \cdot S + w_4 \cdot (1 - M_r/M_0), \quad w_1 + w_2 + w_3 + w_4 = 1$$

Де R_{th} – кількісний показник ризику; t – час після введення PIN-коду; λ – коефіцієнт згасання інформативності теплового сліду; S – коефіцієнт типу клавіатурної панелі; M_0 – початкова кількість пошуку PIN-комбінацій; M_r – залишкова кількість пошуку після врахування теплових слідів; w_1, w_2, w_3, w_4 – вагові коефіцієнти моделі. На відміну від базового підходу, запропонована модель дозволяє кількісно враховувати часові, конструктивні та комбінаторні чинники ризику.

Особливу увагу приділено динамічним клавіатурним панелям, у яких розташування цифр змінюється перед кожним введенням. У такому разі теплова інформація фіксує лише факт натискання певних позицій, але без знання поточної розкладки не забезпечує однозначної відповідності між тепловим слідом і конкретною цифрою. Це істотно знижує імовірність зловмисного розкриття PIN-коду.

У дослідженні виконано порівняння двох підходів, результати якого наведено в таблиці 1.

Таблиця 1. Порівняння підходів та ризиків

Підхід	Інформативність теплових слідів	Вплив на простір пошуку	Переваги	Недоліки
Статична панель	Висока	Суттєве зменшення	Проста реалізація	Найвищий ризик компрометації
Статична панель з маскувальними дотиками	Середня	Помірне зменшення	Не потребує зміни конструкції	Залежить від дисципліни користувача
Матеріали швидкого теплового згасання	Низька або середня	Незначне зменшення	Скорочує час збереження сліду	Потребує зміни конструкції
Динамічна панель	Низька	Мінімальне зменшення	Знижує інформативність слідів	Складніша реалізація

Таблиця 1 демонструє, що найвищий ризик властивий статичним панелям, тоді як динамічні клавіатурні панелі є найбільш ефективним засобом зниження ймовірності компрометації PIN-коду. З цієї таблиці можна зробити висновок який підхід можна використовувати ефективніше всього.

Для порівняння базового та запропонованого підходів у роботі використано рисунок 1, який ілюструє відмінності в оцінюванні ризику витоку інформації через залишкові теплові сліди.

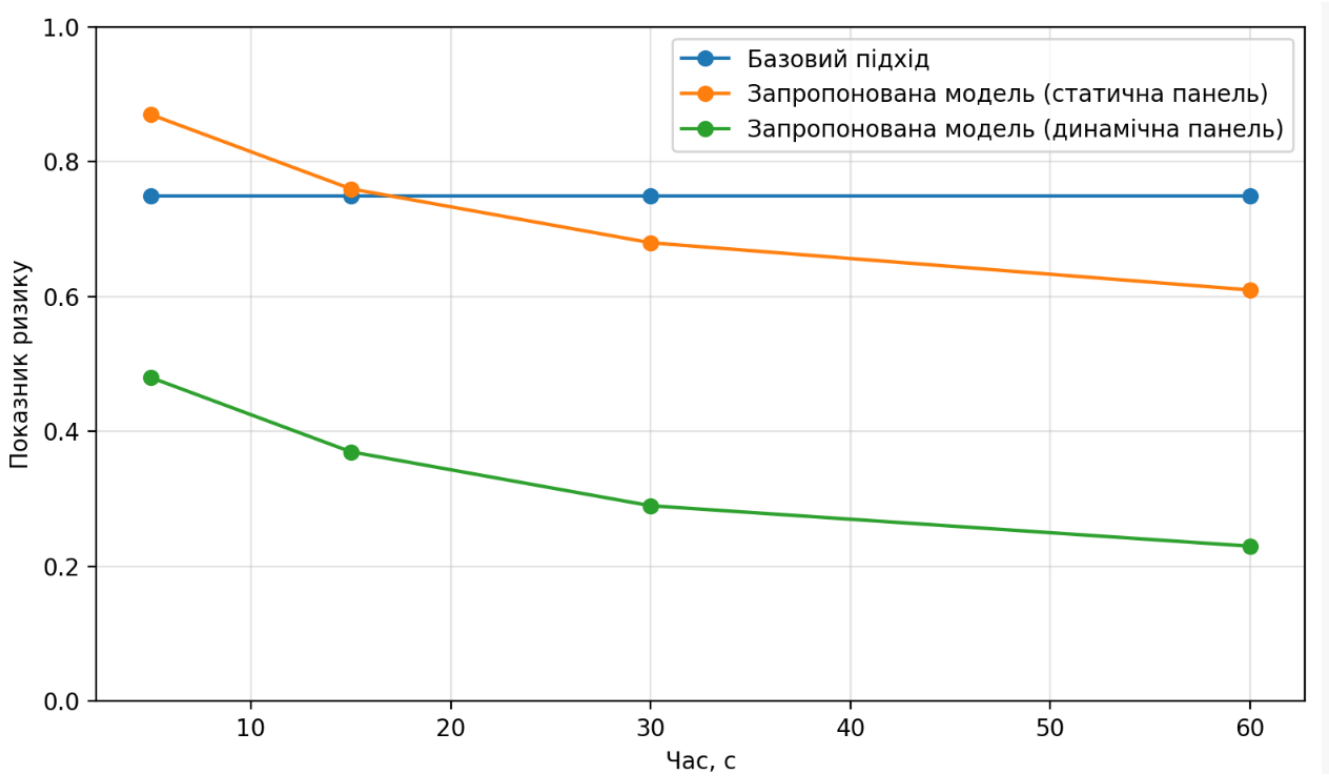

Рис. 1. Графіки показників ризику

На рисунку можна побачити порівняння базового та запропонованого підходу оцінювання ризику витоку інформації PIN-коду через залишкові теплові сліди. Базовий підхід враховує лише кількість виявлених теплових відбитків відносно довжини PIN-коду, тоді як запропонована модель додатково враховує час згасання теплового сліду, тип клавіатурної панелі та залишковий простір пошуку.

Висновки

У результаті проведеного дослідження встановлено, що залишкові теплові сліди на клавіатурних панелях можуть бути реальним побічним каналом витоку інформації під час використання PIN-кодового доступу.

Наукова новизна роботи полягає в удосконаленні підходу до оцінювання ризику витоку інформації через залишкові теплові сліди шляхом одночасного врахування кількості виявлених натискань, часу згасання інформативності сліду, конструктивного типу клавіатурної панелі та показника залишкового простору пошуку PIN-комбінацій а також у введенні кількісного показника ризику.

Практичне значення отриманих результатів полягає в обґрунтуванні доцільності використання динамічних клавіатурних панелей, матеріалів зі зменшеним часом збереження теплового сліду та маскувальних дотиків як засобів зниження ризику витоку інформації. Отримані результати можуть бути використані під час проєктування систем контролю доступу, банківських терміналів і кодових замків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Mowery K., Meiklejohn S., Savage S. Heat of the Moment: Characterizing the Efficacy of Thermal Camera-Based Attacks. Proceedings of the 5th USENIX Workshop on Offensive Technologies, 2011.

2. Wodo W., Hanzlik L. Thermal Imaging Attacks on Keypad Security Systems. Proceedings of SECRYPT, 2016.

3. Marky K., Cherubin G., et al. A User-Centred Design Space to Mitigate Thermal Attacks on Public Payment Terminals. USENIX Security Symposium, 2023.

4. Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. Комплексні системи захисту інформації : навчальний посібник. Вінниця : ВНТУ, 2018. 118 с.

Кохановський Владислав Олександрович - студент, Вінницький національний технічний університет, м. Вінниця, e-mail: 07-23-248.stud@vntu.vn.ua.

Науковий керівник: Гуменюк Вячеслав Володимирович - асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: hvv@vntu.edu.ua.

Kokhanovskyi Vladyslav Oleksandrovych - student, Vinnytsia National Technical University, Vinnytsia,, e-mail: 07-23-248.stud@vntu.vn.ua.

Scientific supervisor: Humeniuk Viacheslav Volodymyrovych - Assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: hvv@vntu.edu.ua.