УДК 004.056

М. М. Маркевич
В. С. Катаєв

РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ЧЕРЕЗ ВІЗУАЛЬНО-ОПТИЧНІ КАНАЛИ НА ОБ'ЄКТАХ ІНФРАСТРУКТУРИ

Вінницький національний технічний університет

Анотація

У роботі розглянуто особливості виникнення та реалізації оптичних каналів витоку інформації на об'єктах інфраструктури. Встановлено, що ключовим вразливим елементом приміщення є віконні прорізи, через які забезпечується можливість дистанційного спостереження без фізичного доступу. Окрему увагу приділено неочевидним загрозам, таким як витік мовної інформації шляхом візуального аналізу артикуляції. Обґрунтовано, що доступність технічних засобів спостереження та простота реалізації оптичних каналів зумовлюють їх широке поширення при недостатньому рівні уваги до них. Запропоновано комплекс організаційних та інженерно-технічних заходів захисту, спрямованих на зниження ризиків несанкціонованого перехоплення інформації.

Ключові слова: оптичний канал витоку інформації, загрози, методи захисту інформації, рекомендації щодо захисту інформації.

Abstract

The paper examines the features of formation and implementation of optical information leakage channels at infrastructure facilities. It is established that window openings represent the key vulnerable element of premises, as they enable remote observation without physical access. Particular attention is paid to non-obvious threats, such as the leakage of speech information through visual analysis of articulation (lip reading). It is substantiated that the availability of technical surveillance means and the simplicity of implementing optical channels contribute to their widespread occurrence despite insufficient attention to associated risks. A set of organizational and engineering-technical protection measures aimed at reducing the risk of unauthorized information interception is proposed.

Keywords: optical channel of information leakage, threats, methods of information protection, recommendations for information protection.

Вступ

Проблема інформаційної безпеки є однією з головних чинників забезпечення належної роботи об'єктів інфраструктури на сьогоднішній день. Зі збільшенням обсягів обробки інформації і активним впровадженням цифрових технологій зростає ймовірність несанкціонованого доступу до інформації, зокрема через технічні канали витоку інформації. Важливе значення мають оптичні канали витоку інформації, що утворюються випромінюванням, перевипромінюванням та відбиванням в інфрачервоній, видимій та ультрафіолетовій областях спектру [1]. Вони становлять загрозу через складність їх виявлення та можливістю перехоплення конфіденційної інформації на відстанях. Метою цього дослідження є аналіз особливостей виникнення оптичних каналів витоку інформації та формування рекомендацій щодо захисту від них на об'єктах інфраструктури.

Результати дослідження

Оптичні канали витоку інформації (ОКВІ) ґрунтуються на можливості перехоплення або аналізу світлового випромінювання, що прямо або опосередковано пов'язане з обробкою конфіденційних даних. До таких каналів належать як прямі оптичні спостереження (через вікна, оптичні прилади, камери відеоспостереження), так і побічні прояви — наприклад, відбиття зображення з екранів моніторів, світлодіодна індикація пристроїв, або зміни освітлення, спричинені роботою обладнання. На відміну від акустичних або віброакустичних каналів, у даному випадку джерелом витоку є саме візуально доступна інформація або її світлові прояви безпосереднього відображення. Основну загрозу становить можливість дистанційного спостереження з використанням оптичного збільшення, цифрової обробки зображень та високочутливих камер, що дозволяє отримувати дані без фізичного проникнення в приміщення [2]. Найбільшу небезпеку ОКВІ становлять саме для візуальних носіїв

інформації — екранів моніторів, проєкційних поверхонь та друкованих документів, оскільки в цих випадках інформація представлена у відкритій, безпосередньо сприйманій формі. Зображення на моніторах і проекторах може бути зчитане як при прямій видимості, так і через відбиття на сторонніх поверхнях (скло, глянцеві меблі), а сучасні оптичні засоби дозволяють відновлювати зміст навіть за частковими або спотвореними відображеннями. Друковані документи, у свою чергу, є статичним джерелом інформації, що значно спрощує їх несанкціоноване фотографування або візуальне копіювання на відстані. Особливо критичним є те, що для реалізації такого витоку не потрібен складний технічний вплив на систему — достатньо забезпечити лінію видимості або використати доступні засоби відеофіксації, що суттєво ускладнює виявлення факту компрометації інформації.

Окрім безпосереднього зчитування візуальної інформації, оптичні канали витоку можуть створювати і менш очевидні загрози, зокрема витік мовної інформації шляхом візуального спостереження за артикуляцією співрозмовників (читання по губах, ліпсинг). За наявності прямої або опосередкованої видимості обличчя людини, сучасні оптичні засоби спостереження у поєднанні з методами обробки зображень дозволяють з достатньою точністю відновлювати зміст розмови навіть без доступу до акустичного сигналу. Така загроза є особливо актуальною під час проведення конфіденційних переговорів у приміщеннях із прозорими або частково прозорими огороджувальними конструкціями, а також у випадках використання відеоспостереження чи відеоконференцзв’язку без належного контролю доступу [3].

Узагальнюючи наведені вище загрози, можна стверджувати, що ключовим вразливим елементом приміщення з точки зору ОКВІ є віконні прорізи, оскільки саме через них у більшості випадків забезпечується можливість дистанційного спостереження без фізичного проникнення, включаючи як пряме візуальне зчитування інформації, так і аналіз її відбиття та побічних оптичних проявів. Реалізація даного каналу зловмисником, як правило, здійснюється шляхом організації прихованого спостереження та відеофіксації об’єкта через доступні лінії видимості. Для цього можуть використовуватись як звичайні засоби відеозйомки (смартфони, цифрові камери), так і спеціалізовані оптичні прилади з функцією збільшення (біноклі, телескопічні об’єктиви), що дозволяє здійснювати зчитування інформації з відстані без привернення уваги. Спостереження може проводитись як у реальному часі, так і з накопиченням відеоматеріалу для подальшого аналізу, зокрема із застосуванням програмних методів підвищення якості зображення, стабілізації, збільшення фрагментів та відновлення частково спотвореної інформації. Додатково можливе використання приховано розміщених камер у суміжних будівлях або транспортних засобах, що забезпечує тривале та малопомітне спостереження за об’єктом без необхідності безпосереднього доступу до приміщення. Додатково слід враховувати, що спостереження та відеофіксація можуть ефективно здійснюватися і в умовах обмеженої освітленості або в нічний час із використанням приладів нічного бачення та тепловізійних засобів, які дозволяють виявляти силуети, рухи та теплові контури об’єктів, розширюючи тим самим часові межі реалізації ОКВІ.

Попри те, що оптичні канали є одними з найбільш поширених через відсутність потреби у дороговартісному спеціалізованому шпигунському обладнанні та високій кваліфікації зловмисника, на практиці їм часто не приділяється належної уваги, що призводить до недооцінки ризиків і підвищення ймовірності компрометації інформації. Відповідно, для того щоб уникнути таких загроз необхідно використовувати певні методи захисту від оптичних каналів, які в основному є організаційними та інженерно-технічними [4].

Першочерговим заходом захисту від даних каналів є забезпечення ефективного контролю доступу до приміщення, що передбачає обмеження перебування сторонніх осіб у зонах обробки конфіденційної інформації, впровадження пропускного режиму, використання систем ідентифікації та автентифікації, а також ведення обліку відвідувачів. Такий підхід дозволяє мінімізувати ризики несанкціонованого візуального спостереження безпосередньо всередині приміщення, зокрема через використання мобільних пристроїв, портативних камер або інших засобів відеофіксації.

Наступним важливим заходом є раціональне розміщення робочих місць та технічних засобів обробки інформації, зокрема моніторів, проєкційних екранів і робочих столів з документами, таким чином, щоб виключити їхню видимість через віконні прорізи або інші потенційні точки зовнішнього спостереження. Рекомендується орієнтувати екрани перпендикулярно до вікон, уникати їх розташування навпроти світлопрозорих конструкцій, а також враховувати можливість непрямих відбиттів на поверхнях інтер’єру. Такий підхід дозволяє суттєво знизити ймовірність зчитування інформації як при прямому спостереженні, так і через опосередковані оптичні прояви.

Важливим елементом захисту також є використання штор, жалюзі або інших світлозахисних засобів на віконних прорізах, які дозволяють обмежити або повністю виключити можливість зовнішнього візуального спостереження. Застосування таких рішень забезпечує контроль прозорості вікон залежно від умов освітлення та режиму роботи, а також створює додатковий бар'єр для прямого і опосередкованого зчитування інформації ззовні приміщення.

Отже, розглянуті рекомендації щодо захисту оптичних каналів витоку інформації на об'єктах інфраструктури дозволяють запобігти несанкціонованому перехопленню важливої інформації.

Висновки

У результаті проведеного дослідження встановлено, що оптичні канали витоку інформації є суттєвим фактором загрози для об'єктів інфраструктури, оскільки забезпечують можливість дистанційного несанкціонованого доступу до конфіденційних даних без фізичного проникнення в приміщення. Визначено, що основними джерелами витоку виступають візуальні носії інформації, зокрема екрани технічних засобів, проєкційні поверхні та друковані документи, а ключовим вразливим елементом приміщення є віконні прорізи, через які реалізується більшість сценаріїв спостереження. Показано, що простота реалізації таких каналів та доступність засобів відеофіксації зумовлюють їх широке поширення при одночасній недооцінці рівня небезпеки. Запропоновані організаційні та інженерно-технічні заходи, зокрема контроль доступу до приміщень, раціональне розміщення джерел візуальної інформації та використання світлозахисних засобів, дозволяють суттєво знизити ризики витоку інформації. Отримані результати можуть бути використані при проєктуванні та вдосконаленні систем захисту інформації на об'єктах інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Горліченко С. ОСОБЛИВОСТІ ФОРМУВАННЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ ВІД СУЧАСНИХ ІКС. Ukrainian Scientific Journal of Information Security. 2023. Т. 29, № 2. С. 80–87. URL: https://doi.org/10.18372/2225-5036.29.17872 (дата звернення: 24.03.2026).
2. Loughry J., Umphress D. A. Information leakage from optical emanations. ACM Transactions on Information and System Security. 2002. Vol. 5, no. 3. P. 262–289. URL: https://doi.org/10.1145/545186.545189 (date of access: 25.03.2026).
3. An optical covert-channel to leak data through an air-gap / M. Guri et al. 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12–14 December 2016. 2016. URL: https://doi.org/10.1109/pst.2016.7906933 (date of access: 25.03.2026).
4. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 25.03.2026).

Маркевич Мар'яна Михайлівна – студентка групи 1БКС-23б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: 7mariaanaa@gmail.com

Катаєв Віталій Сергійович – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: kataev@vntu.net

Mariana Markevych – student of group 1BKS-23b, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: 7mariaanaa@gmail.com

Vitalii Kataiev – assistant of the Department of Management and Security of Information Systems; Vinnytsia National Technical University, Vinnytsia, e-mail: kataev@vntu.net