Державна служба
спеціального зв'язку та захисту
інформації України

КОНТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Системи технічного захисту інформації



Інформаційний бюлетень
ISSN 3154-8814 (print)

№ 2 ◦ 2026

Державна служба
спеціального зв'язку та захисту
інформації України

Інформаційний бюлетень №2

КОНТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

системи технічного захисту інформації

виходить щомісяця

2026

УДК 001.92(051)

КОНТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ:

системи технічного захисту інформації

Інформаційний бюлетень №2 • 2026

Редакційна колегія:

Головний редактор: д-р техн. наук, професор Олександр ПОТІЙ, Держспецзв'язку.

Заступник головного редактора: д-р юрид. наук, професор Володимир ТРОФИМЕНКО, Держспецзв'язку.

Відповідальний редактор: д-р техн. наук, професор Володимир ПАВЛІКОВ, ДержНДІ технологій кібербезпеки.

Технічний редактор: д-р техн. наук, доцент Семен ЖИЛА, ДержНДІ технологій кібербезпеки.

Члени редакційної колегії:

ДержНДІ технологій кібербезпеки: Дмитро БОНДАРЕНКО; канд. техн. наук Олександр ДИРДА; Сергій ЛИСЕНКО; Ігор НАВРОЦЬКИЙ; канд. техн. наук Максим КОМАРОВ; Максим ІЩУК; канд. геогр. наук Микола ДОБИШ.

Департамент захисту інформації Адміністрації Держспецзв'язку: Михайло РИБКА; Микола СНІЖИНСЬКИЙ; Олександр ЧЕРНАЧУК.

Департамент цифрової трансформації Адміністрації Держспецзв'язку: Наталя ДОРОФЄЄВА.

Департамент кіберзахисту Адміністрації Держспецзв'язку: Олександр МАТВІЙЧУК-ЮДІН.

Державний центр кіберзахисту Держспецзв'язку: Артем ЖИЛІН.

Управління з кіберзахисту інформаційно-комунікаційних систем Адміністрації Держспецзв'язку: Віталій БЕЗШТАНЬКО.

Департамент протидії технічним розвідкам та інструментального контролю стану захисту інформації Адміністрації Держспецзв'язку: Вадим СИВКО; Сергій БЕЗВЕРХИЙ; Василь БАРЧЕНКО.

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) – державний орган, який призначений для забезпечення функціонування та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, активної протидії агресії у кіберпросторі, а також інших завдань відповідно до закону.

Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації (ДержНДІ технологій кібербезпеки) – провідна науково-дослідна установа Держспецзв'язку, яка реалізує науково-технічні завдання у сферах криптографічного та технічного захисту інформації, розроблення і впровадження новітніх технологій кібербезпеки в інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності, а також технологій протидії технічним засобам розвідки.

Департамент захисту інформації Адміністрації Держспецзв'язку відповідає за реалізацію державної політики у сфері захисту інформації, забезпечуючи безпеку даних в державних інформаційних системах та об'єктах критичної інфраструктури.

ISSN 3154-8814 (print)

© Державна служба спеціального зв'язку та захисту інформації України, 2026

© Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, 2026

Зміст

ВСТУП 5

УМОВНІ СКОРОЧЕННЯ 8

НОРМАТИВНО-ПРАВОВЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ТЗІ 9

Оновлений перелік засобів технічного захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України 10

Актуалізовано версію повного переліку нормативних документів системи технічного захисту інформації 12

Затверджено нормативний документ НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» 15

НАУКОВІ ІНТЕРВ'Ю ПРО ПРИХОВАНІ КАНАЛИ В ТЕХНІЧНОМУ ЗАХИСТІ ІНФОРМАЦІЇ 19

Як штучний інтелект навчився відновлювати текст із побічних електромагнітних випромінювань HDMI 21

Як побічні електромагнітні випромінювання вбудованих камер перетворюються на канал візуального шпигунства 26

Як електромагнітні випромінювання IoT-пристроїв можуть перетворитися на новий інструмент цифрової криміналістики 33

Як оптичні побічні випромінювання повернули стару TEMPEST-проблему в нову цифрову епоху 39

Як нелінійне розсіяння в оптичному волокні дозволяє знаходити підслуховувача з точністю до сантиметрів 44

Як гнучка п'єзоелектрична структура перетворюється на активний бар'єр проти витоку мовної інформації через вібрації 50

Як технічні канали витоку через побічні електромагнітні випромінювання змушують по-новому дивитися на захист інформації 56

Як мінімізація взаємної інформації перетворює штучний шум на точний інструмент протидії витоку побічними каналами 63

Як відремонтований USB-кабель клавіатури відкриває несподіваний TEMPEST-канал витоку 68

Як нова теорема про побічні канали витоку в зашифрованому трафіку змінює саму логіку захисту 74

Як побічні електромагнітні випромінювання комп'ютера дозволяють відновлювати зображення без доступу до самого дисплея 79

Як правильний вибір рівня сигналу дозволяє залишити зв'язок усередині контрольованої зони й одночасно позбавити противника можливості перехоплення 84

Як VGA\HDMI – кабель перетворюється на передавач, а звичайні LoRa-шлюзи – на приймачі прихованого витоку 89

Як звичайний диференціальний датчик тиску перетворюється на засіб витоку інформації акустичним канал і дозволяє відновлювати мовну інформацію? 96

Як сучасне глибоке навчання перетворює звук натискань на практичний канал витоку навіть через смартфон і Zoom 103

СУЧАСНІ НАУКОВІ ДОСЛІДЖЕННЯ ТА ТЕНДЕНЦІЇ РОЗВИТКУ ТЗІ 110

Аналіз сучасних наукових досліджень та публікацій у сфері технічного захисту інформації 111

Акустичні канали витоку інформації під час натискання клавіш клавіатури 111

Сучасні методи аналізу побічних каналів, що застосовуються для атак на криптографічні реалізації алгоритму AES 113

Витік фінформації через електромагнітні випромінювання сенсорних екранів 115

Акустичні побічні сигналів для забезпечення безпеки промислових роботизованих систем 116

Методи підвищення ефективності екранування ПЕМВН електронної техніки 117

Ефективний захист 3D-принтерів від акустичних side-channel атак шляхом модифікації G-code 120

Створення прихованого каналу витоку даних з air-gapped систем через компрометуючі випромінювання кабелів 121

Аналіз акустичного витоку від звичайних комп'ютерних мишей 122

Аналіз нової вразливості у відремонтованих USB-кабелях клавіатур 123

Тренд 2025–2026: Deep-TEMPEST (застосування машинного навчання для відновлення зображень за побічними електромагнітними випромінюваннями інтерфейсу HDMI) та посилення активного зашумлення периферійних пристроїв 126

Вступ

Сучасний розвиток інформаційних систем супроводжується зростанням ролі технічного захисту інформації як ключового елементу забезпечення безпеки державних інформаційних ресурсів та інформації з обмеженим доступом. Ускладнення архітектур обчислювальних систем, розширення спектра використовуваних технічних засобів та підвищення рівня інтеграції цифрових технологій зумовлюють появу нових каналів витоку інформації, зокрема побічних електромагнітних випромінювань і наводок, акустичних та віброакустичних проявів, а також їх комбінованих форм. У цих умовах забезпечення належного рівня захищеності вимагає не лише застосування сучасних технічних засобів, але й формування цілісної нормативно-технічної бази, здатної адекватно відображати поточні загрози та забезпечувати їх ефективну нейтралізацію.

Актуальність досліджуваної проблематики визначається необхідністю забезпечення стійкого функціонування інформаційних систем в умовах постійної експлуатації та динамічної зміни загроз. Особливого значення набуває питання уніфікації підходів до вибору, застосування та оцінювання заходів технічного захисту інформації, що дозволяє забезпечити відтворюваність результатів оцінки захищеності та виключити суб'єктивність при прийнятті технічних рішень. У цьому контексті важливим є формування єдиної системи нормативних документів, яка встановлює вимоги до параметрів захисту, методів випробувань і процедур оцінювання відповідності.

Однією з ключових умов ефективного функціонування систем технічного захисту інформації є наявність актуалізованої номенклатури засобів, що підтвердили відповідність встановленим вимогам. Регулярне оновлення переліків таких засобів забезпечує можливість їх застосування без додаткових процедур перевірки за умови дотримання визначених умов експлуатації. При цьому технічні характеристики засобів, зокрема параметри затухання сигналів, рівні шумових завад, чутливість вимірювальних пристроїв та точність визначення електромагнітних полів, виступають основою для кількісної оцінки ефективності захисту від витоку інформації технічними каналами. Встановлення граничних значень цих параметрів дозволяє забезпечити контроль за неможливістю відновлення інформації за межами контрольованих зон.

Паралельно з розвитком технічної складової відбувається вдосконалення процедурного забезпечення вибору заходів

захисту. Сучасні підходи базуються на структурованій класифікації заходів, яка передбачає їх поділ на класи, групи та рівні посилення залежно від результатів оцінки ризиків. Такий підхід забезпечує адаптацію систем захисту до конкретних умов експлуатації, включаючи типи оброблюваної інформації, особливості об'єктів інформаційної діяльності та характер потенційних технічних каналів витоку. Визначення мінімально допустимих параметрів налаштування та їх фіксація в технічній документації створює передумови для подальшої об'єктивної перевірки ефективності реалізованих заходів.

Важливим етапом забезпечення захищеності є оцінювання достатності реалізованих заходів технічного захисту інформації. Застосування комплексного підходу, що поєднує аналіз документації, опитування персоналу та проведення експериментальних випробувань, дозволяє отримати всебічну характеристику функціонування систем захисту. Така багаторівнева процедура оцінювання сприяє виявленню невідповідностей між задекларованими та фактичними параметрами, а також забезпечує документальне підтвердження досягнутого рівня захищеності. У результаті формується обґрунтована основа для прийняття рішень щодо відповідності інформаційних систем встановленим вимогам.

Суттєвий вплив на розвиток технічного захисту інформації здійснюють сучасні наукові дослідження, присвячені аналізу побічних фізичних каналів витоку. Результати таких досліджень демонструють, що акустичні сигнали, електромагнітні випромінювання та інші фізичні прояви роботи технічних засобів можуть містити значний обсяг інформативних ознак, придатних для відновлення оброблюваних даних. Використання методів машинного навчання, зокрема згорткових і рекурентних нейронних мереж, дозволяє автоматизувати процес виділення характерних патернів і значно підвищити ефективність аналізу побічних сигналів. Це призводить до появи нових класів загроз, що потребують відповідного вдосконалення засобів протидії.

Особливого значення набуває тенденція до комбінованого використання різних фізичних каналів витоку, що забезпечує підвищення точності відновлення інформації за рахунок інтеграції взаємодоповнювальних сигналів. Поєднання акустичних і електромагнітних даних, а також застосування алгоритмів їх зваженого об'єднання дозволяє підвищити співвідношення сигнал–шум і скоротити обсяг необхідних спостережень для досягнення заданого рівня точності. У свою чергу, це обумовлює необхідність комплексного підходу до захисту, який враховує всі можливі фізичні канали витоку та їх взаємодію.

Поряд із розвитком методів технічної розвідки активно вдосконалюються засоби протидії, зокрема технології екранування та активного зашумлення. Використання сучасних композитних матеріалів, що поєднують властивості поглинання та відбиття електромагнітних хвиль, дозволяє суттєво зменшити рівень побічних випромінювань та радіус небезпечної зони. Інтеграція таких матеріалів у конструкції електронної техніки, а також застосування генераторів шуму нового покоління створюють додаткові бар'єри для перехоплення інформації. Водночас впровадження алгоритмічних методів маскування, зокрема модифікації керуючих програм технічних пристроїв, відкриває нові можливості для захисту від акустичних каналів витоку.

Сучасні тенденції розвитку галузі свідчать про перехід до використання інтелектуальних методів як у реалізації атак, так і у побудові систем захисту. Концепції, що базуються на застосуванні глибинного навчання для аналізу електромагнітних еманацій, демонструють здатність відновлювати зображення та текстову інформацію з високим рівнем точності. Це підвищує вимоги до параметрів екранування, фільтрації сигналів та організації контрольованих зон, а також стимулює розвиток нових підходів до виявлення та нейтралізації подібних загроз.

Таким чином, сучасний стан технічного захисту інформації визначається взаємодією трьох ключових складових: нормативно-технічного регулювання, технічних засобів та наукових досліджень. Їх узгоджений розвиток забезпечує формування ефективної системи протидії витоку інформації технічними каналами, здатної адаптуватися до нових викликів та забезпечувати належний рівень захищеності в умовах постійного вдосконалення інформаційних технологій.

Умовні скорочення

ТЗІ – технічний захист інформації

НД ТЗІ – нормативний документ системи технічного захисту інформації

ПЕМВН – побічні електромагнітні випромінювання і наводки

AES – Advanced Encryption Standard (стандарт симетричного шифрування)

air-gapped – ізольована (фізично відокремлена від мереж) система

ASIDS – Acoustic Side-channel Intrusion Detection System (система виявлення вторгнень на основі акустичних побічних каналів)

BER – Bit Error Rate (ймовірність бітової помилки)

CNN – Convolutional Neural Network (згорткова нейронна мережа)

COTS – Commercial Off-The-Shelf (комерційно доступні готові рішення)

GnuPG – GNU Privacy Guard (програмна реалізація криптографічних алгоритмів)

HDMI – High-Definition Multimedia Interface (інтерфейс передавання цифрового відео та аудіо)

HID – Human Interface Device (пристрій введення користувача)

IoT – Internet of Things (Інтернет речей)

LoRa – Long Range (технологія бездротового зв'язку великої дальності)

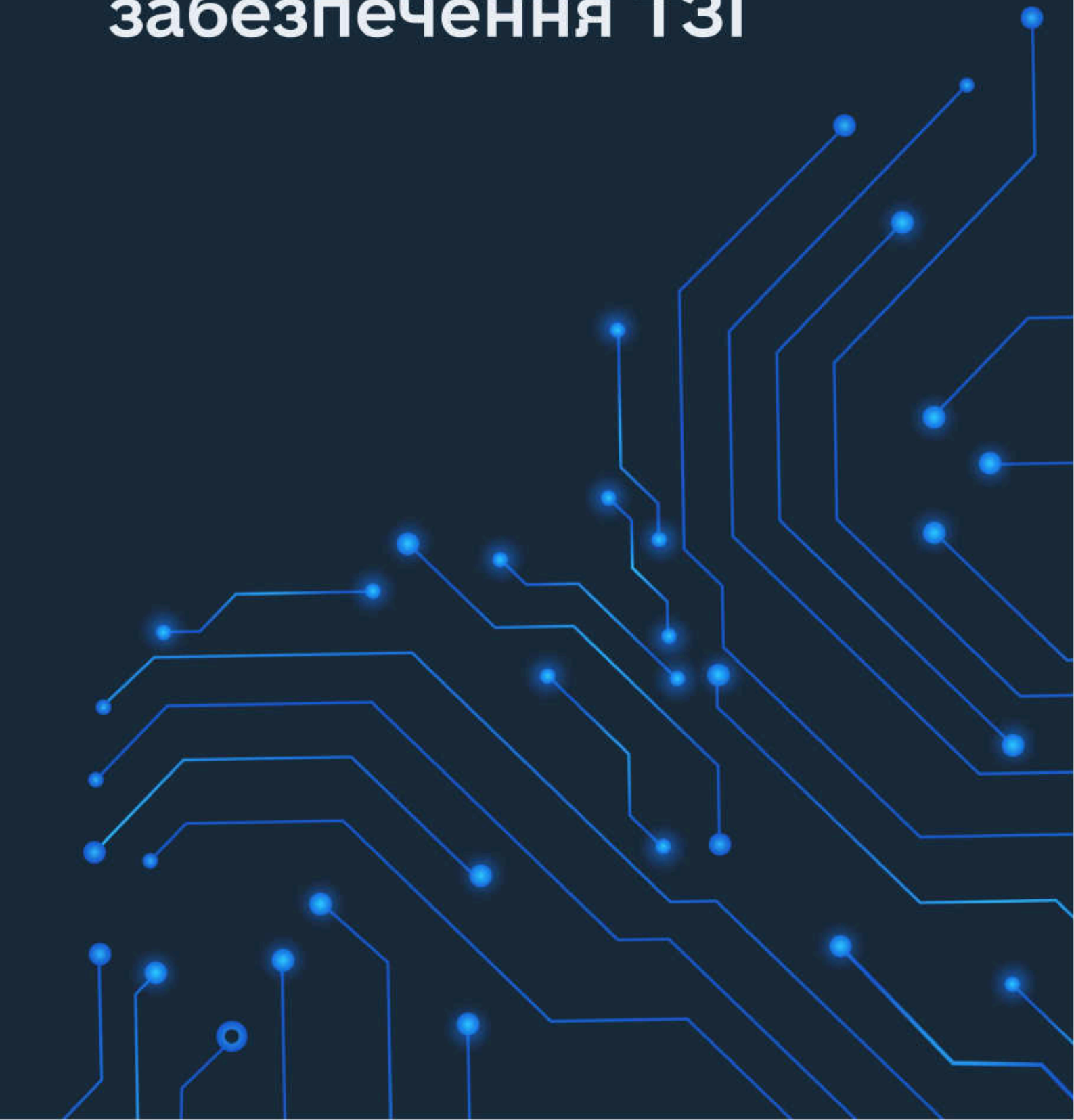
ML – Machine Learning (машинне навчання)

NATO – North Atlantic Treaty Organization (Організація Північноатлантичного договору)

RSA – Rivest–Shamir–Adleman (алгоритм асиметричного шифрування)

USB – Universal Serial Bus (універсальна послідовна шина)

Нормативно-правове та організаційне забезпечення ТЗІ



Оновлений перелік засобів технічного захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України

> У грудні 2025 року Адміністрація Державної служби спеціального зв'язку та захисту інформації України оприлюднила оновлений **перелік засобів технічного захисту інформації,** дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Файл **Perelik_Zasobiv_TZI_2025-12-18.ods** розміщено на порталі відкритих даних відповідно **до пункту 17 Положення про технічний захист інформації в Україні**. Оновлення переліку проведено шляхом внесення змін до попередньої редакції з урахуванням **нових позитивних експертних висновків**, отриманих за результатами **державної експертизи**. Перелік містить **номенклатуру засобів**, основним функціональним призначенням яких є **захист інформації від загроз витоку технічними каналами, порушення цілісності та блокування**. До нього включено також засоби, в яких додатково до основного призначення передбачено **функції технічного захисту інформації**, засоби, спеціально розроблені або пристосовані для **пошуку закладних пристроїв**, та засоби, спеціально розроблені або пристосовані для **оцінювання захищеності інформації**.

Процедура включення засобів до оновленого переліку базується на **підтвердженні відповідності вимогам нормативних документів системи технічного захисту інформації сертифікатом відповідності** або **позитивним експертним висновком**. Експертні висновки видаються відповідно до **Положення про державну експертизу у сфері технічного захисту інформації та Правил проведення робіт із сертифікації засобів захисту інформації**. Для засобів, строки дії експертних висновків яких завершилися після **24 лютого 2022 року**, дія продовжено **до закінчення воєнного стану**. Це забезпечує **безперервне застосування засобів на об'єктах інформаційної діяльності** без необхідності повторної експертизи в умовах обмежених ресурсів. Оновлений перелік формується **щоквартально**, з вилученням засобів, що втратили відповідність, та включенням нових, які пройшли випробування на відповідність **граничним значення параметрів витоку інформації**.

> Забезпечує	Оновлення переліку в грудні 2025 року забезпечує актуальну технічну базу для проведення робіт з технічного захисту інформації на об'єктах, де циркулює інформація з обмеженим доступом.

Засоби першої категорії призначені для **приховування мовної інформації в телефонних лініях** та **захисту від акустичних** і **віброакустичних каналів витоку**. Їх технічні характеристики включають **коефіцієнти затухання сигналів та рівень генерації спеціальних сигналів**, що перевіряються під час випробувань на відповідність встановленим граничним значення. Засоби другої категорії охоплюють **радіовиявлювачі вимірювальні, індикаторні та аналізувальні**, параметри яких включають **чутливість, діапазон частот та похибку вимірювання напруженості електромагнітного поля**. Випробування таких засобів проводяться з фіксацією параметрів у **контрольованій зоні** для забезпечення неможливості відновлення інформації за межами цієї зони.

Засоби третьої категорії включають **пристрої для пошуку закладних пристроїв**, методика розробки яких передбачає **аналіз конструктивних особливостей** та проведення **контрольних вимірювань у реальних умовах експлуатації об'єкта**. Четверта категорія охоплює **засоби оцінювання захищеності**, що дозволяють проводити **кількісну оцінку залишкових параметрів витоку** після застосування заходів захисту. Включення засобів до переліку вимагає подання виробником **протоколів приймальних випробувань, технічної документації та результатів державної експертизи**. Після включення засоби можуть застосовуватися без додаткової атестації комплексу за умови дотримання умов експлуатації, визначених у технічній документації.

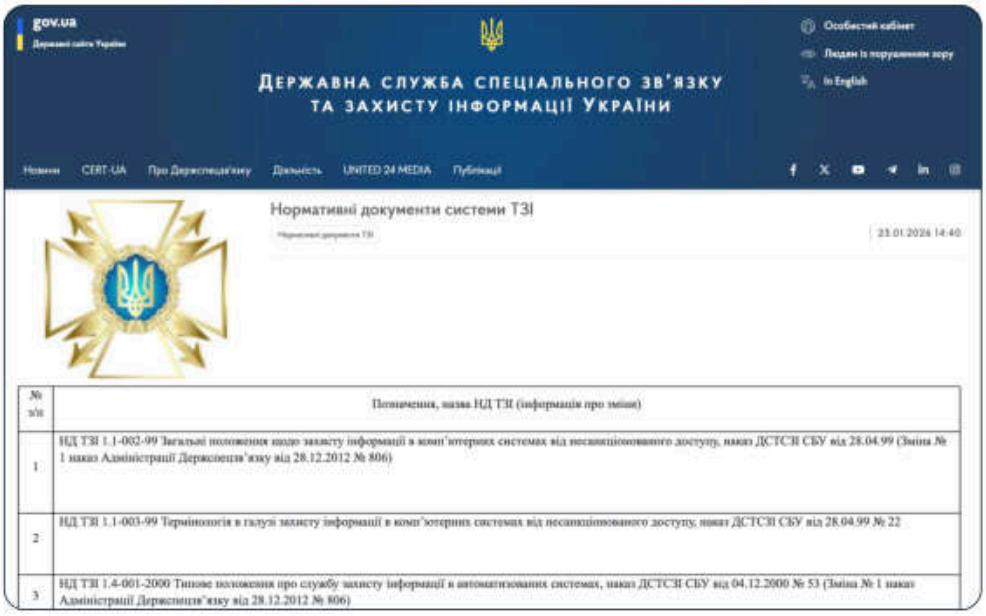
Оновлення переліку в грудні 2025 року забезпечує **уніфікацію номенклатури** для всіх суб'єктів, що здійснюють технічний захист інформації, незалежно від відомчої належності об'єктів.

Адміністрація Держспецзв'язку. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. wd.clarity-project.info/resource/60e016f2-4733-4149-90f0-e3214a710481

Актуалізовано версію повного переліку нормативних документів системи технічного захисту інформації

У січні 2026 року на офіційному ресурсі оприлюднено актуалізовану версію повного переліку нормативних документів системи технічного захисту інформації. Публікація відбулася 23 січня 2026 року та містить **40 документів** з точними позначеннями, назвами, датами затвердження та примітками щодо змін (Рисунок 1). Перелік нормативних документів включає як базові положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, так і спеціалізовані методики випробувань радіовиявлювачів вимірювальних, індикаторних та аналізувальних.

Сайт Держспецзв'язку з переліком нормативних документів системи ТЗІ



До нього внесено актуальні редакції документів, що регулюють порядок створення комплексних систем захисту інформації, класифікацію автоматизованих систем та вимоги до захисту інформації на веб-сторінках. Публікація забезпечує єдину технічну базу для всіх робіт з технічного захисту інформації, дозволяючи суб'єктам перевіряти відповідність застосовуваних засобів поточним нормативним вимогам без пошуку окремих документів [1].

Актуалізований перелік нормативних документів у січні 2026 року включає документи, що встановлюють правила побудови, викладення та оформлення нормативних документів системи технічного захисту інформації, положення про категоріювання об'єктів інформаційної діяльності та класифікатор засобів технічного захисту інформації. Кожен документ

супроводжується посиланням на наказ про затвердження та змінами, внесеними в попередні роки. Публікація переліку дозволяє проводити роботи з технічного захисту інформації за єдиними правилами, включаючи оцінку захищеності від витоку каналами побічних електромагнітних випромінювань і наводок та акустичними каналами. Оновлення переліку нормативних документів забезпечує сумісність засобів технічного захисту інформації з вимогами до автоматизованих систем різних класів та об'єктів, де обробляється інформація з обмеженим доступом.

Паралельно з оновленням нормативної бази в грудні 2025 року оприлюднено план проведення конференцій на 2026 рік, до якого включено Всеукраїнську студентську науково-практичну **конференцію «Технічний захист інформації 2026»**. Конференція запланована на 9–11 грудня 2026 року на базі факультету комп'ютерних наук і технологій Національного авіаційного університету. Мета конференції – обмін результатами наукових досліджень у галузі технічного захисту інформації між студентськими колективами. Конференція передбачає розгляд практичних аспектів застосування оновлених засобів технічного захисту інформації та нормативних документів у автоматизованих системах. Організатори визначили технічний фокус на методах випробувань засобів виявлення закладних пристроїв та оцінці захищеності від витоку технічними каналами. План конференції на 2026 рік забезпечує продовження науково-практичної діяльності, спрямованої на вдосконалення технічного захисту інформації. [2]

Оновлення переліку засобів технічного захисту інформації в грудні 2025 року та публікація переліку нормативних документів у січні 2026 року формують замкнутий цикл забезпечення технічної бази. Перелік засобів безпосередньо пов'язаний з нормативними документами, оскільки включення до нього можливе лише після підтвердження відповідності вимогам цих документів. Такий підхід усуває розбіжності між практичним застосуванням засобів та нормативними вимогами, дозволяючи проводити оцінку захищеності з використанням кількісних параметрів, таких як коефіцієнт приховування інформації, рівень затухання сигналів та поріг чутливості радіовиявлювачів. Для радіовиявлювачів вимірювальних класів актуальні вимоги встановлюють граничні значення похибки вимірювання напруженості поля в діапазоні частот, що відповідають характеристикам типових джерел випромінювання. Для засобів пасивного приховування мовної інформації уточнено методику розрахунку ефективності загороджувальних фільтрів з урахуванням частотних характеристик сигналів.

Публікація оновленого переліку засобів у грудні 2025 року забезпечує можливість вибору засобів для конкретних технічних каналів витоку інформації без додаткових перевірок. Засоби активного захисту мовної інформації класифікуються за потужністю джерел та рівнем шумів у приміщенні, що дозволяє адаптувати їх до об'єктів різного об'єму. Радіовиявлювачі аналізувальні класи забезпечують розрахунок ймовірності виявлення закладних пристроїв з урахуванням рівня шумів у приміщенні. Оновлення переліку нормативних документів у січні 2026 року інтегрується з цим процесом, надаючи єдину термінологію та структуру для опису заходів захисту. Це дозволяє проводити роботи з технічного захисту інформації за єдиними правилами, незалежно від відомчої належності об'єкта.

Конференція «Технічний захист інформації 2026», запланована на грудень 2026 року, стане продовженням наукової підтримки оновленої нормативної бази. Участь студентських колективів дозволить представити результати аналізу методик випробувань радіовиявлювачів та засобів захисту мовної інформації після застосування оновленого переліку засобів. План конференції передбачає акцент на оновлених версіях засобів технічного захисту інформації та їх відповідності актуальним нормативним документам. Така науково-практична діяльність забезпечує передачу знань щодо застосування оновленого переліку засобів та нормативних документів у реальних умовах експлуатації об'єктів інформаційної діяльності.

Таким чином, події грудня 2025 року – січня 2026 року щодо оновлення переліку засобів технічного захисту інформації та публікації переліку нормативних документів демонструють системне вдосконалення технічного захисту інформації.

> Відповідність Оновлення забезпечують точність оцінки захищеності від витоку технічними каналами, уніфікацію номенклатури засобів та відповідність експертних висновків вимогам нормативних документів системи технічного захисту інформації.

Це створює умови для стабільного функціонування засобів технічного захисту інформації в автоматизованих системах, де обробляється інформація з обмеженим доступом, відповідно до вимог актуальної нормативної бази.

1. Нормативні документи системи ТЗІ
   cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024
2. Всеукраїнська студентська науково-практична конференція «Технічний захист інформації 2026»
   nau.edu.ua/ua/event/2026/vseukrainska-studentska-naukovo-praktichna-konferentsiya-tehnichniy-zahist-informatsii-2026.html

Затверджено нормативний документ НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем»

Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30 квітня 2024 року № 234 затверджено нормативний документ **НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем»**. Цей документ встановлює єдину процедуру вибору заходів технічного захисту інформації в інформаційних системах, де обробляється інформація з обмеженим доступом. Процедура базується на структурованому підході до класифікації заходів, де кожний захід поділяється на групи та можливі посилення залежно від рівня загроз витоку технічними каналами. Вибір здійснюється з урахуванням результатів попередньої оцінки ризиків та специфіки об'єкта інформаційної діяльності, що забезпечує адаптацію захисту до реальних умов експлуатації.

Документ визначає двадцять класів заходів технічного захисту, кожен з яких охоплює групи дій з безпеки інформації. Для кожного класу передбачено базові дії, які можуть бути посилені додатковими функціональними можливостями або підвищеними параметрами налаштування. Посилення застосовуються у випадках, коли базовий рівень захисту недостатній за результатами розрахунку залишкових ризиків витоку. Параметри налаштування заходів мають мінімально необхідні значення, які не підлягають послабленню; ці значення фіксуються в технічній документації системи та перевіряються під час оцінки захищеності. Такий підхід дозволяє формувати цільовий профіль захисту з урахуванням конкретних технічних каналів витоку інформації, включаючи побічні електромагнітні випромінювання, наводки та акустичні канали, без використання універсальних шаблонів.

У липні 2024 року Адміністрація Державної служби спеціального зв'язку та захисту інформації України видала наказ від 10 липня 2024 року, яким затверджено Рекомендації з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних системах. Рекомендації встановлюють порядок проведення оцінки реалізації заходів,

вибраних відповідно до НД ТЗІ 3.6-006-24. Оцінка проводиться за трьома основними методами: дослідженням документації та налаштувань, опитуванням персоналу, відповідального за експлуатацію засобів технічного захисту, та випробуванням функціональних механізмів захисту в реальних умовах експлуатації. Кожен метод має визначену глибину та охоплення, що фіксується в звіті про оцінку.

Процедура оцінки базового рівня захисту починається з перевірки відповідності обраних заходів мінімальним вимогам, встановленим у НД ТЗІ 3.6-006-24. Для кожного заходу **фіксується висновок** щодо його реалізації: позитивний або негативний, з обґрунтуванням на підставі фактичних параметрів налаштування. Оцінка цільового рівня захисту здійснюється з урахуванням результатів базового рівня та додаткових вимог, що випливають з аналізу технічних каналів витоку на конкретному об'єкті. Якщо оцінка дає позитивний результат за обома рівнями, це стає підставою для декларування відповідності комплексної системи захисту інформації вимогам технічного захисту. Рекомендації передбачають можливість використання засобів технічного захисту інформації, що не пройшли державну експертизу, за умови обов'язкового обґрунтування їх вибору та проведення додаткових випробувань на відповідність граничним значенням параметрів витоку.

Оновлення нормативної бази продовжилося в грудні 2025 року та січні 2026 року публікацією актуалізованої версії повного переліку нормативних документів системи технічного захисту інформації на офіційному інформаційному ресурсі. До переліку внесено НД ТЗІ 3.6-006-24 та оновлені частини НД ТЗІ 2.3-025-24 (у трьох томах), які конкретизують методику оцінювання заходів захисту для інформаційних систем. Публікація забезпечує єдність технічної бази для всіх суб'єктів, що здійснюють роботи з технічного захисту інформації. Новий документ НД ТЗІ 3.6-006-24 інтегрується з процедурами оцінки, викладеними в Рекомендаціях від 10 липня 2024 року, утворюючи замкнутий цикл: вибір заходів – їх реалізація – оцінка достатності – декларування відповідності.

Технічні наслідки застосування НД ТЗІ 3.6-006-24 проявляються в можливості точного налаштування параметрів захисту для кожного класу заходів. Наприклад, у класах, що стосуються управління доступом, параметри включають тривалість сеансу, кількість невдалих спроб авторизації та періодичність перевірки активності облікових записів. Ці параметри фіксуються в описі **цільового профілю захисту** та перевіряються під час оцінки методом випробувань. Аналогічно, для класів, пов'язаних із захистом від витоку технічними

каналами, встановлюються граничні значення затухання сигналів та рівня перешкод, що безпосередньо впливають на ефективність засобів пасивного та активного приховування інформації. Такий детальний підхід усуває суб'єктивність при виборі засобів технічного захисту та забезпечує відтворюваність результатів оцінки захищеності.

Рекомендації від 10 липня 2024 року деталізують структуру звіту про оцінку. Звіт містить розділи, присвячені кожному методу оцінки, з таблицями висновків за конкретними заходами. Для методу дослідження фіксуються факти наявності документації на заходи захисту та відповідність налаштувань мінімальним параметрам. Метод опитування дозволяє верифікувати знання персоналу щодо процедур експлуатації засобів технічного захисту. Метод випробувань передбачає проведення контрольних тестів на відповідність граничним значенням параметрів витоку в контрольованій зоні. Позитивна оцінка за всіма методами є підставою для оформлення декларації відповідності системи технічного захисту інформації.

У січні 2026 року після оприлюднення оновленого переліку нормативних документів суб'єкти, що здійснюють технічний захист інформації, отримали можливість використовувати НД ТЗІ 3.6-006-24 як основу для формування індивідуальних методик вибору заходів. Це оновлення усуває розбіжності між попередніми підходами до створення комплексних систем захисту та сучасними вимогами до адаптивності захисту. Процедура вибору заходів тепер включає обов'язковий етап аналізу вхідних даних, таких як результати попередньої оцінки ризиків та специфіка оброблюваної інформації. На підставі цих даних формується перелік класів заходів, для кожного з яких визначається базовий рівень та необхідні посилення.

Оновлення, внесені в 2024–2026 роках, забезпечують перехід **від статичного** застосування засобів технічного захисту інформації **до динамічного процесу**, де вибір і оцінка заходів здійснюються на підставі кількісних параметрів. НД ТЗІ 3.6-006-24 встановлює єдину термінологію та структуру опису заходів, що спрощує взаємодію між розробниками та експертами під час державної експертизи. Рекомендації від 10 липня 2024 року, у свою чергу, стандартизують процес оцінки достатності, роблячи його відтворюваним і документально підтвердженим. Разом ці документи формують нову технічну базу для проведення робіт з технічного захисту інформації в інформаційних системах, де обробляється інформація з обмеженим доступом.

Публікація оновленої версії нормативних документів у грудні 2025 – січні 2026 років завершує цикл нормативного забезпечення. Тепер усі суб'єкти мають доступ до єдиної

актуальної бази, що включає НД ТЗІ 3.6-006-24 та Рекомендації з оцінки достатності. Це дозволяє проводити роботи з технічного захисту інформації за єдиними правилами, незалежно від відомчої належності об'єкта. Технічні вимоги до параметрів налаштування та методів оцінки забезпечують об'єктивність висновків щодо захищеності від витоку інформації технічними каналами.

Таким чином, оновлення, затверджені наказами Адміністрації Державної служби спеціального зв'язку та захисту інформації України в 2024 році та оприлюднені в 2025–2026 роках, **формують сучасну нормативно-технічну базу** для вибору та оцінки заходів технічного захисту інформації. НД ТЗІ 3.6-006-24 та Рекомендації з оцінки достатності заходів встановлюють чіткі процедури, параметри та методи, що забезпечують підвищення точності та відтворюваності робіт з технічного захисту інформації без використання застарілих підходів. Ці зміни спрямовані на забезпечення стабільного захисту інформації від витоку технічними каналами в умовах постійної експлуатації інформаційних систем.

Наказ Адміністрації Держспецзв'язку від 30.04.2024 №234 «Про внесення змін до нормативного документа системи технічного захисту інформації НД ТЗІ 3.6-006-21»
cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-30-04-2024-234-pro-vnesennya-zmin-do-normativnogo-dokumenta-sistemi-tekhnichnogo-zakhistu-informaciyi-nd-tzi-3-6-006-21

Наукові інтерв'ю про приховані канали в технічному захисті інформації



Наукові інтерв'ю про приховані канали в технічному захисті інформації

канд. техн. наук Олександр ШМАТКО,
Департамент захисту інформації Адміністрації Держспецзв'язку

У цьому розділі матеріали подано у форматі віртуальних інтерв'ю між читачем і авторами наукових статей. Такий формат дозволяє не просто переказати зміст публікацій, а показати їхню логіку, головні результати, практичне значення та приховані ризики у зрозумілішій формі.

У кожному матеріалі читач ставить авторам запитання, які природно виникають під час знайомства з темою: у чому суть роботи, що саме доведено, чому це важливо, які межі методу, де практична загроза і які висновки випливають для сфери ТЗІ. У відповідях збережено наукову основу першоджерел, але подано її в більш доступному, журнальному стилі – без втрати змісту, фактів і технічної ваги.

Отже, далі на читача чекає не сухий перелік статей, а послідовна розмова з дослідниками: про акустичні, оптичні, електромагнітні та волоконно-оптичні канали витоку, про нові методи перехоплення, виявлення й протидії, а також про те, як сучасна наука змінює саме уявлення про межі спостережуваності інформації. Це формат, у якому складні речі читаються як бесіда, але залишаються серйозним аналітичним матеріалом.

Як штучний інтелект навчився відновлювати текст із побічних електромагнітних випромінювань HDMI [1]

Екран комп'ютера здається замкненим світом: що з'явилося на дисплеї, те бачить лише користувач. Але сучасна електроніка майже ніколи не працює мовчки. Разом із корисним сигналом вона залишає побічні сліди – слабкі, фонові, на перший погляд хаотичні. Саме в цих слідах і криється одна з найцікавіших тем сучасного технічного захисту інформації: чи можна відновити зображення на екрані, не підключаючись до самого пристрою, а лише аналізуючи його ненавмисні електромагнітні випромінювання? Стаття Deep-TEMPEST: Using Deep Learning to Eavesdrop on HDMI from its Unintended Electromagnetic Emanations дає на це тривожну відповідь: так, і значно краще, ніж це вдавалося раніше.

Назва вашої роботи звучить майже провокаційно. Ви справді показали, що з HDMI можна відновлювати інформацію з екрана?

Так. Ми досліджували побічні електромагнітні випромінювання, які виникають під час передавання відеосигналу через HDMI. Ідея полягає в тому, що ці випромінювання містять непряму, але не нульову інформацію про вміст зображення. Наше завдання було не просто зафіксувати сам факт витоку, а показати, що сучасні алгоритми можуть використати такі сигнали для значно кращого відновлення тексту, ніж це робили попередні TEMPEST-інструменти.

Але HDMI – це ж цифровий інтерфейс. Чому з ним узагалі можлива така атака?

Саме цифрова природа HDMI і робить задачу складною. У старих аналогових інтерфейсах зв'язок між сигналом і зображенням був прямішим. У випадку HDMI використовується TMDS-кодування, де сигнал набагато складніший, а залежність між перехопленим випромінюванням і пікселями екрана є нелінійною. Через це традиційні підходи часто дають лише розмиті та майже нечитабельні результати. Але складність сигналу не означає, що його не можна використати – особливо якщо залучити моделі глибокого навчання.

У чому тоді головна відмінність вашого підходу?

Ми запропонували перестати дивитися на задачу як на просте «очищення» зіпсованої картинки. Натомість ми розглянули її як обернену задачу: маючи деградований комплексний сигнал, відновити початкове зображення. Для цього ми використали глибоку нейронну мережу, яка працює не лише з амплітудою сигналу, а з його комплексними відліками, тобто з амплітудою і фазою одночасно. Це принципово важливо, бо саме тут прихована частина інформації, яку попередні методи відновлення інформації просто втрачали.

Чому фаза настільки важлива?

Тому що вона теж несе структуру сигналу. Якщо брати лише модуль, як це часто робилося в попередніх реалізаціях, частина інформативності безповоротно втрачається. У наших експериментах модель, яка використовувала комплексні значення, показала кращий результат, ніж модель, що працювала тільки з амплітудою. Для реальних даних CER становив 35,3% для комплексного підходу проти 43,6% для варіанта лише з модулем, тоді як звичайний підхід давав близько 92,2% CER.

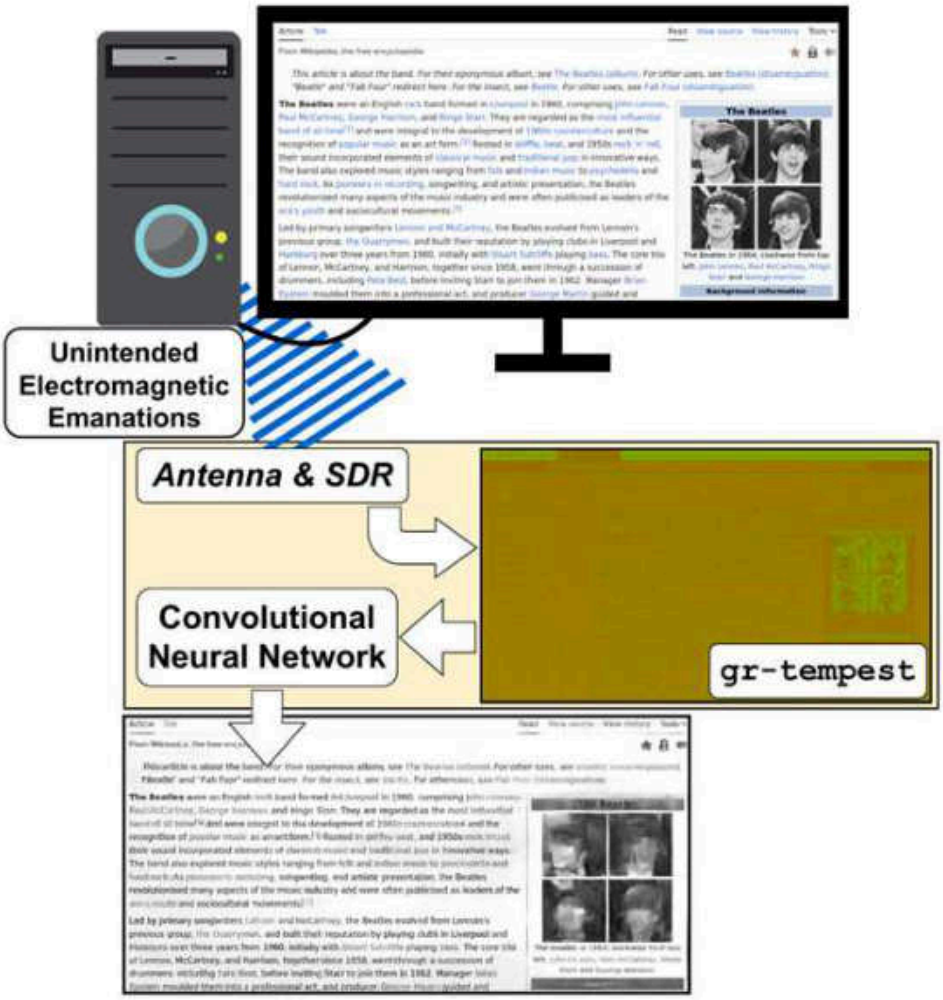
Тобто йдеться вже не просто про шум, а про текст, який реально можна прочитати?

Саме так. Ми спеціально зосередилися на тексті, оскільки в більшості практичних сценаріїв саме текстова інформація становить найбільшу цінність. Ми оцінювали результати через Character Error Rate (CER) – тобто дивилися, наскільки текст, отриманий після реконструкції, відрізняється від оригіналу. І побачили, що навіть там, де традиційні методи майже безсилі, новий підхід дозволяє зробити текст набагато читабельнішим.

Як виглядає така система в реальному експерименті?

Вона не потребує екзотичної апаратури. У нашій роботі використовувалися антена, SDR-приймач, фільтрація, підсилення і комп'ютер для обробки

сигналів. Ненавмисні випромінювання від HDMI-кабелю та роз'ємів приймаються антеною, після чого SDR формує комплексні відліки. Далі ці дані обробляються системою на базі GNU Radio та нейронної мережі, яка намагається відновити вихідне зображення. Схема цього процесу показана на рисунку.



Запропонована система. Кабель HDMI та роз'єми випромінюють ненавмисні електромагнітні сигнали, які фіксуються SDR та обробляються gr-tempest, отримуючи деградоване комплекснозначне зображення, яке, у свою чергу, подається на згорткову нейронну мережу для визначення вихідного зображення. Усі три зображення відповідають фактичним результатам.

Багато хто сказав би: навіщо така складна математика, якщо можна просто натренувати нейромережу на прикладах?

Тому що без фізичної моделі нейромережа перетворюється на чорну скриньку без керованості. Нам було важливо зрозуміти, як формується сигнал HDMI-випромінювання, на яких гармоніках зосереджується його енергія і на які частоти доцільно налаштовувати SDR. Саме аналітична модель дозволила не лише пояснити природу сигналу, а й

згенерувати синтетичні навчальні дані, що значно зменшило залежність від довгих і складних натурних вимірювань.

Тобто ви навчали модель не тільки на реальних сигналах?

Так. І це один із сильних результатів роботи. Ми сформували набір із 3491 пар «чисте зображення – деградоване спостереження», з яких 1302 були реальними, а решта – симульованими. Ми також показали, що попереднє навчання на синтетичних даних і подальше донавчання на відносно невеликій кількості реальних прикладів дає дуже сильний результат. Зокрема, fine-tuning після синтетичного навчання дозволяв досягати якості, близької до повного навчання на реальних даних, використовуючи лише частину реальної вибірки.

А наскільки практично небезпечні ваші результати? 35% помилки – це вже серйозно?

Для абстрактної задачі розпізнавання це могло б виглядати як недосконалий результат. Але в TEMPEST-сценарії це вже дуже суттєво. Коли текст частково відновлений, людина часто здатна дочитати решту за контекстом. Тобто навіть неповна реконструкція може становити реальний ризик витоку конфіденційної інформації. Саме тому ми вважаємо, що межа між «нечитабельним шумом» і «достатньо інформативним сигналом» сьогодні змінилася.

Чи означає це, що старі критерії оцінки побічних випромінювань уже застарівають?

Принаймні вони потребують перегляду. Раніше можна було припустити: якщо сигнал дуже спотворений, то практичної загрози немає. Наша робота показує, що це вже не завжди так. Сучасні алгоритми, особливо моделі глибокого навчання, здатні добувати інформацію навіть із дуже деградованих спостережень. Отже, оцінювати потрібно не лише фізичний рівень витоку, а й те, що сучасна обробка сигналів здатна з нього реконструювати.

Наскільки універсальний ваш метод? Чи спрацює він для будь-якого монітора і будь-якого режиму?

Не повністю. Ми побачили, що система має певну робастність, наприклад до зміни гармоніки налаштування SDR. Але зміна роздільної здатності монітора вже може істотно погіршити результат. Це означає, що для нових конфігурацій потрібне або додаткове донавчання, або окреме налаштування моделі. І саме тут знову стають важливими симуляції, які дозволяють масштабувати підхід на нові умови.

Який головний висновок із вашої публікації?

Побічні електромагнітні випромінювання HDMI, які раніше могли виглядати як занадто слабкі, спотворені чи малоінформативні, у поєднанні з SDR та глибоким навчанням стають значно небезпечнішим джерелом витоку, ніж це здавалося раніше.

Чому це важливо вже сьогодні

У цій історії найбільш тривожним є не сам факт існування побічних випромінювань – про них відомо давно. Справжня зміна відбулася в іншому: те, що вчора виглядало як технічний фон, сьогодні дедалі частіше стає відновлюваним сигналом. Штучний інтелект не створив TEMPEST-загрози, але різко знизив поріг її практичного використання. І саме тому сучасний технічний захист інформації має враховувати не лише фізику витоку, а й обчислювальну силу того, хто цей витік аналізує.

Висновок

Монітор більше не є лише пристроєм відображення. У цифрову епоху він може стати джерелом побічної інформації, а сучасні алгоритми – інструментом її повернення з майже невидимого сліду. Дослідження Deep-TEMPEST показує просту, але принципову річ: у світі, де штучний інтелект навчився реконструювати зміст із шуму, саме поняття «достатньо захищено» потребує нового переосмислення.

Як побічні електромагнітні випромінювання вбудованих камер перетворюються на канал візуального шпигунства [2]

Ми звикли думати, що камера – це пристрій, який просто дивиться на світ. Але в цифровій електроніці спостереження майже ніколи не залишається безслідним. Щойно сенсор фіксує сцену, зображення починає рухатися всередині пристрою – рядок за рядком, піксель за пікселем, біт за бітом. І на цьому шляху інформація може ненавмисно «просочуватися» назовні у вигляді електромагнітних випромінювань. Саме це показує стаття EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras: вбудовані камери здатні випромінювати достатньо структурований сигнал, щоб за певних умов сторонній спостерігач міг відновлювати зображення.

Ваша робота звучить майже як сюжет технотрилера. Ви справді показали, що з камери можна «зняти» зображення, не маючи доступу до її мережі чи пам'яті?

Так. Ми дослідили не програмні, а фізичні побічні канали витоку. Ідеться про електромагнітні випромінювання, які виникають під час передавання цифрових даних від сенсора камери до процесора обробки зображення. Ми показали, що ці сигнали можуть містити достатньо інформації, щоб відновлювати потік зображень із вбудованих камер. Саме цю вразливість ми назвали EM Eye.

Чому ця тема настільки важлива саме зараз?

Тому що камери отримали велике розповсюдження. Вони є у смартфонах, домашніх системах спостереження, розумних замках, автомобільних реєстраторах та багатьох інших вбудованих системах. Такі пристрої часто працюють у приватних просторах і можуть фіксувати дуже чутливу інформацію. При цьому більшість попередніх досліджень зосереджувалися на програмних або мережевих загрозах, а не на фізичному рівні апаратури. Ми вирішили подивитися на проблему з іншого боку: чи може сама робота камери створювати канал витоку.

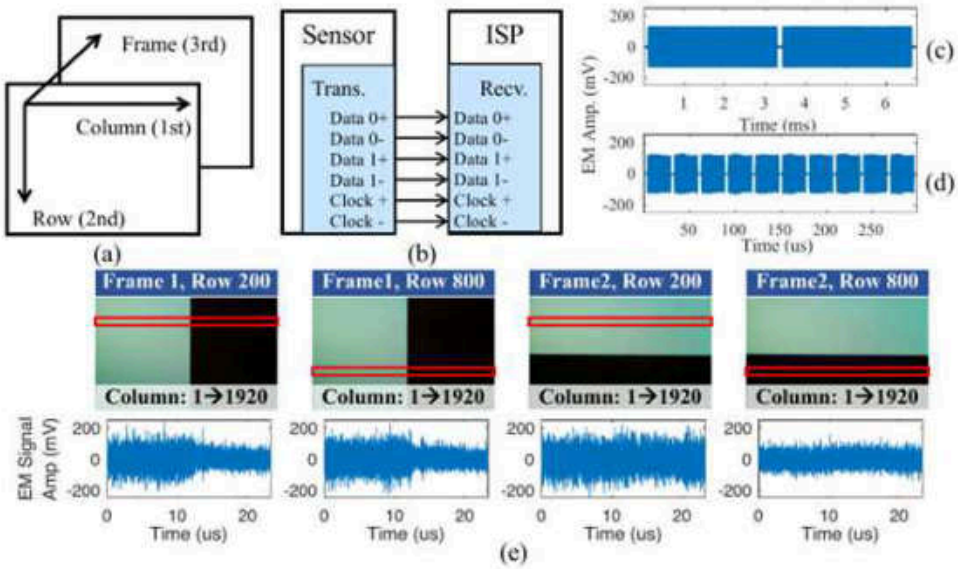
У чому полягає фізичне джерело цього витоку?

Основне джерело – інтерфейс передавання даних між сенсором зображення та наступними компонентами обробки, зокрема ISP або GPU. Камера формує сирі RAW-дані, які передаються у строго визначеному порядку: кадр за кадром, рядок за рядком, піксель за пікселем. Під час цієї цифрової передачі по дротах виникають електромагнітні випромінювання. Саме кабель або лінії передавання даних фактично поводяться як ненавмисна передавальна антена.

Тобто дані з камери не просто «витікають», а ще й мають чітку структуру?

Саме так. Це не хаотичний шум. Наші експерименти показали чіткі кореляції між формою електромагнітного сигналу і вмістом зображення. Ми спостерігали періодичність на рівні кадрів, рядків і навіть фрагментів усередині рядків. Саме ця структурованість і робить відновлення зображення принципово можливим. На рисунку статті це добре видно: електромагнітні сигнали змінюються відповідно до різних кадрів, рядків і колонок зображення.

Як робота вбудованих камер генерує електромагнітні сигнали, що призводять до витоку інформації про зображення з камери.



(a) Кожен відеокадр передається рядок за рядком і стовпець за стовпцем. (b) Інтерфейс MIPI CSI-2 передає дані зображення за допомогою кількох ліній диференціальних проводів даних та проводів тактової частоти, що генерує витік електромагнітних сигналів. (c) Електромагнітні сигнали двох послідовних кадрів. (d) Електромагнітні сигнали десяти послідовних рядків. (e) Електромагнітні сигнали передачі різних кадрів, рядків та стовпців, що демонструють чітку кореляцію зі вмістом зображення.

Які саме камери виявилися вразливими?

Ми перевірили чотири популярні платформи розробки з камерами, зокрема Raspberry Pi, Nvidia Jetson Nano та Asus Tinkerboard, а також 12 комерційних пристроїв із камерами. Серед них були смартфони, домашні камери спостереження і автомобільні реєстратори. Ми побачили, що проблема не обмежується якоюсь однією моделлю чи одним виробником – це значно ширший клас вразливості.

Наскільки далеко може перебувати атакуючий?

Це залежить від типу пристрою, довжини та екранування кабелю, а також від антени. Для смартфонів максимальні відстані в наших вимірюваннях були невеликими – від 1 до 30 сантиметрів, що більше відповідає сценарію прихованої близької антени. Для домашніх камер і відеореєстраторів відстані були суттєво більшими: у низці випадків – до 3,5–5 метрів. Саме тому для частини пристроїв ми вважаємо реалістичним сценарій спостереження через стіну, двері або вікно.

Як виглядає така атака на практиці?

Ми розглядали два сценарії. Перший – hidden-antenna, коли невелика антена встановлюється близько до камери, наприклад у модифікованому аксесуарі або поруч із пристроєм. Другий – physical-isolation, коли камера перебуває у фізично ізольованому просторі, а приймальна система розташована зовні. Для збирання сигналів використовуються антена, малошумний підсилювач, SDR-приймач і ноутбук із програмною обробкою.

Ви пишете, що це схоже на TEMPEST-атаки проти дисплеїв. У чому різниця?

Фізичний принцип схожий: незахищене цифрове передавання зображення випромінює назовні електромагнітний слід. Але для камер задача складніша. У дисплейних атаках часто мішенню були прості сцени – текст на однорідному фоні. Камерні

сцени набагато різноманітніші: обличчя, кімнати, предмети, світлові градієнти, складні текстури. Через це спотворення в реконструкції стають помітно серйознішими, а проблема вимагає глибшого моделювання. Автори прямо зазначають, що вразливість камер і дисплеїв має спільну фізичну основу, але між класичним розумінням TEMPEST і сучасними сенсорними системами існує семантичний розрив.

Що саме заважає отримати ідеальне зображення?

Головна проблема – обмеження практичного приймання. Атакувальник зазвичай не може зняти весь цифровий спектр передавання, який може мати порядок гігагерц. Типові SDR і ноутбуки працюють із значно вужчими смугами, наприклад близько 8–10 МГц. Через це втрачається частина структури цифрових даних. Наслідком стають характерні спотворення: втрата кольору, переплутане відображення відтінків сірого, світлові градієнти, контуроподібні артефакти та високочастотний шум. Ці ефекти показані й пояснені в статті.

Тобто прямої реконструкції недостатньо?

Так. Базовий підхід дозволяє відновити структуру сцени в реальному часі, але з вираженими спотвореннями. Тому ми запропонували розширений підхід: спочатку формується односмугова реконструкція, далі – багатосмугове комбінування для зменшення спотворень, а потім застосовується модель image-to-image translation на базі pix2pix, яка вчиться переводити реконструйоване зображення у вигляд, ближчий до реального виходу камери.

Чому вам знадобилася нейромережа?

Тому що спотворення мають не випадковий, а структурований характер. Наприклад, яскраві ділянки можуть у реконструкції перетворюватися на темні полігони, а однорідні поверхні – вкриватися штучними градієнтами. Людина, дивлячись на таке зображення, часто інтуїтивно «домислює» правильну сцену. Ми поставили питання: чи можна автоматизувати це за

допомогою моделі, яка навчиться відповідності між спотвореними ЕМ-зображеннями і справжніми кадрами. Експерименти показали, що так – і якість відновлення від цього зростає дуже суттєво.

Як ви оцінювали якість?

Ми використали не лише класичні візуальні метрики на кшталт SSIM, а й прикладні показники, які краще відображають зміст сцени. Для набору зображень із людьми ми рахували face detection rate – наскільки добре на реконструкції визначаються обличчя. Для інтер'єрних сцен – indoor scene captioning rate, тобто наскільки схожими є текстові описи, згенеровані для реконструкції і для оригіналу. Це дозволяє оцінювати не тільки «красу картинки», а й реальну інформативність витоку.

І наскільки великим було покращення?

На наборах із різними оптичними матрицями та контролерами ми спостерігали дуже значні прирости порівняно з базовими сучасними підходами прямої реконструкції. Для варіантів із донавчанням під конкретні комбінації оптичної матриці та контролера прирости були ще більшими.

Що найбільше впливає на силу витоку?

Дуже багато залежить від кабелю. Екранування реально допомагає: у наших тестах захисні матеріали на кшталт провідної тканини або алюмінієвої фольги знижували рівень побічного сигналу приблизно на 9,84 дБ і 14,33 дБ відповідно. Але навіть за таких умов деяка реконструкція все ще залишалася можливою. Також важливі довжина кабелю, відстань до антени і її орієнтація. Довші кабелі часто випромінювали ефективніше, а отже дозволяли перехоплення з більшої дистанції.

Ви згадуєте смартфони, домашні камери й автомобільні реєстратори. Які сценарії атаки ви вважаєте найреалістичнішими?

Для смартфонів – сценарій прихованої антени недалеко від пристрою. Автори наводять приклад модифікованого павербанка або спільного зарядного пристрою, у якому може бути захована приймальна система. Для домашніх камер і реєстраторів більш реалістичними виглядають атаки з за перешкоди, наприклад: через стіну, двері, вікно або ззовні автомобіля чи приміщення. Саме тому ці категорії пристроїв викликають особливе занепокоєння.

Який головний технічний висновок вашої роботи?

Головний висновок у тому, що конфіденційність систем відео реєстрації не можна оцінювати лише на рівні програмного доступу. Дані можуть «витікати» ще до того, як вони потраплять в операційну систему чи мережу, – на рівні фізичного передавання всередині пристрою. І якщо це передавання не має достатнього захисту, камера може перетворитися на ненавмисний передавач зображення.

А що це означає для розробників і фахівців із захисту інформації?

Що захист систем відео реєстрації треба розглядати комплексно. Необхідно звертати увагу на протоколи передавання даних, екранування, фізичну компоновку, довжину кабелів, баланс між вартістю і безпекою. Автори прямо пишуть, що їхня модель може допомагати не лише атакувальникам, а й захисникам – для ідентифікації витоку та удосконаленням протоколів передавання з мінімальними витратами.

Чому це важливо вже зараз

Найнеприємніше в цій історії те, що камера тут не «ламається» в класичному сенсі. Вона просто працює так, як була спроєктована, – і саме ця нормальна робота породжує небажаний побічний слід. Стаття EM Eye показує, що сучасний ризик витоку даних у вбудованих системах більше не обмежується програмними вразливостями. Інколи достатньо того, що пристрій бачить світ і оброблює картинку всередині себе. А все інше за нього вже зроблять антена, SDR і хороша модель реконструкції.

Фінальний висновок

Камера давно перестала бути просто «оком» пристрою. У цифрову епоху вона стала ще й джерелом побічної телеметрії про приватний простір. Дослідження EM Eye показує тривожну, але дуже важливу річ: у світі сенсорів інформація може витікати ще до того, як її хтось «зламає» на рівні програмного коду. І тому справжній захист майбутнього починається не з паролів і шифрування, а з розуміння того, як самі фізичні процеси всередині пристрою перетворюються на мову, яку вміє читати сучасна електронна розвідка.

Як електромагнітні випромінювання IoT-пристроїв можуть перетворитися на новий інструмент цифрової криміналістики [3]

У цифровій криміналістиці довгий час головними джерелами доказів були жорсткі диски, мобільні телефони та мережеві журнали. Але світ змінився. Розумні годинники, камери, медичні імпланти, голосові асистенти, домашні датчики й безліч інших IoT-пристроїв увійшли в повсякденне життя – а разом із ним і в поле зору слідчих. Проблема лише в тому, що ці пристрої часто побудовані на нестандартному апаратному та програмному забезпеченні, через що класичні методи вилучення цифрових доказів або не працюють, або вимагають руйнівного втручання. Саме на цьому тлі дисертація Electromagnetic Side-Channel Analysis Methods for Digital Forensics on Internet of Things пропонує незвичний, але сильний хід: використовувати побічні електромагнітні випромінювання не для атаки, а як неінвазивне джерело криміналістичних відомостей про внутрішній стан IoT-пристрою.

У чому головна ідея вашої роботи?

Головна ідея полягає в тому, що електромагнітний побічний канал можна використати не лише як інструмент атаки, а й як інструмент цифрової криміналістики. Я досліджував, чи можливо за допомогою аналізу побічного електромагнітного випромінювання отримувати корисні відомості з IoT-пристроїв у неінвазивний спосіб, особливо там, де класичні методи вилучення цифрових доказів не працюють або є занадто ризикованими.

Чому саме IoT-пристрої створюють таку проблему для криміналістики?

Тому що вони надзвичайно різноманітні й часто не мають стандартних інтерфейсів для дослідження. На відміну від персональних комп'ютерів або навіть смартфонів, багато IoT-пристроїв побудовані на спеціалізованих мікроконтролерах, мають нестандартні прошивки, незвичні формати зберігання або взагалі не зберігають дані локально. Через це традиційний підхід – зняти образ пам'яті й аналізувати його – часто стає неможливим або потребує руйнівних процедур, як-от chip-off чи SEM-аналіз.

Тобто ви пропонуєте дивитися не всередину мікросхеми, а на те, що вона випромінює назовні?

Саме так. Будь-який електронний пристрій, який працює, випромінює електромагнітну енергію. Ці випромінювання часто містять структуровану інформацію про те, що саме пристрій робить у конкретний момент. Якщо навчитися правильно їх реєструвати та інтерпретувати, можна отримати відомості про криптографічні операції, версію прошивки, ознаки шкідливих змін у апаратній частині або навіть поточний внутрішній стан пристрою. Саме це і стало предметом дослідження.

У чому тут криміналістична відмінність?

Різниця в меті. Аналізуючи побічні електромагнітні випромінювання зазвичай прагнуть отримати секрет, наприклад ключ шифрування. У криміналістичному контексті завдання інше: не обов'язково витягти весь секретний вміст, а отримати надійні, корисні для розслідування ознаки поведінки пристрою. Наприклад, чи виконувався певний криптографічний алгоритм, яка саме версія апаратної частини працює, чи була вона змінена, у якому стані перебуває IoT-система. Це вже не просто атака, а спосіб неінвазивного інструментального спостереження.

Які саме питання ви поставили у своїй роботі?

Дослідження побудоване навколо трьох головних питань. Перше – які EM-SCA-методи взагалі здатні давати корисні криміналістичні інсайти з IoT-пристроїв. Друге – як зробити ці методи достатньо ефективними, щоб ними можна було користуватися не лише в лабораторії, а й у практичних умовах. І третє – як впоратися з різноманіттям IoT-екосистеми, де майже кожен тип пристрою потребує свого підходу. Саме з цих трьох питань і виросла вся архітектура дисертації.

Ви не просто описали ідею, а створили ще й практичний інструмент?

Так. У межах дисертації було запропоновано модель IoT-криміналістики на основі EM-SCA і реалізовано у вигляді відкритого програмного фреймворку EMvidence. Його ідея полягає в модульності: окремі модулі відповідають за конкретні типи пристроїв і конкретні види криміналістичних інсайтів. Це дозволяє не концентрувати всю складність в одному універсальному інструменті, а розподіляти її між окремими мінімалістичними модулями.

Чому така модульність настільки важлива?

Тому що світ IoT надто різноманітний. Один пристрій – це мікроконтролер із BLE, інший – камера з SoC, третій – сенсор із власним протоколом. Неможливо створити один жорстко зашитий метод, який однаково добре працюватиме для всіх. Тому EMvidence побудовано за логікою Unix-філософії: невеликі спеціалізовані модулі, кожен з яких виконує конкретне завдання. Така архітектура краще переносить зміни ринку IoT.

Які саме інсайти вдалося отримувати з електромагнітних випромінювань?

У дисертації показано, що з EM-випромінювань можна з високою точністю виявляти криптографічні події, визначати версію firmware, помічати шкідливі модифікації в прошивці, а також розпізнавати поточний внутрішній стан IoT-пристрою. У роботі прямо сказано, що машинне навчання дозволяло автоматично ідентифікувати відомі патерни випромінювання з точністю понад 90% у відповідних сценаріях.

Отже, машинне навчання стало центральним елементом?

Так, без нього практична придатність такого підходу була б набагато нижчою. Для криміналіста неприйнятно, щоб результат залежав від глибокого ручного аналізу спектрограм фахівцем із радіотехніки. Тому в роботі наголос зроблено саме на ML-методах, які автоматизують розпізнавання EM-патернів і знижують поріг входу для практичного застосування. EMvidence замислювався саме як платформа, де такі

моделі можна інтегрувати у зрозумілий слідчий програмний пакет. Але EM-дані зазвичай дуже великі.

Хіба це не робить метод занадто важким для польових умов?

Саме це було одним із ключових викликів. У роботі окремо досліджується проблема ефективності. Високі частоти дискретизації та велика ширина смуги роблять EM-дані об'ємними і важкими для обробки на ноутбуках чи польових станціях. Тому я дослідив два підходи до зменшення обчислювального навантаження: по-перше, зниження частоти дискретизації до межі, де це ще не шкодить точності, і, по-друге, інтелектуальний вибір інформативних каналів. Було показано, що зменшення частоти дискретизації може скоротити обсяг даних до 80%, а вибір 500 вимірів із 20 000 різко знижує розмірність без критичної втрати інформативності. Це дуже важливий момент.

Ви фактично кажете, що side-channel аналіз можна зробити польовим інструментом?

Саме до цього і вела робота. Ідея полягала не в тому, щоб створити суто академічну демонстрацію, а в тому, щоб показати: навіть на помірно ресурсних комп'ютерах, які слідчі можуть мати під час огляду, такий підхід може бути корисним. Звісно, не йдеться про повну заміну всіх класичних методів. Але як альтернативне вікно в ситуаціях, коли звичайний доступ до даних заблокований, EM-SCA може стати дуже сильним доповненням.

А які саме пристрої ви досліджували?

У роботі як приклади використовувалися, зокрема, Raspberry Pi 3 B+ та Arduino Leonardo, а також розглядався ширший контекст IoT-пристроїв із мікроконтролерами, радіомодулями, сенсорами й актуаторами. Це не означає, що метод вичерпується цими платформами. Навпаки, вони були вибрані як репрезентативні для моделювання ширшого спектра реальних IoT-систем. У дисертації є важливий юридичний підтекст.

Наскільки взагалі такий підхід придатний з точки зору судової допустимості?

Це один із найважливіших аспектів. У цифровій криміналістиці недостатньо просто щось виявити – потрібно, щоб спосіб отримання даних можна було документувати, пояснити й захистити в суді. Саме тому в дисертації велика увага приділена не лише технічним методам, а й загальній моделі процесу: від планування збору даних до формування звіту. EMvidence у цьому сенсі виступає не просто як інструмент аналізу, а як основа для відтворюваного й структурованого процесу криміналістичного огляду.

Які головні обмеження ви самі визнаєте?

Їх кілька. По-перше, робота не розглядає пристрої, які вже мають активні апаратні чи програмні контрзаходи протидії витоку. По-друге, хоча використані експериментальні платформи є репрезентативними, майбутні дослідження мають ширше охоплювати комерційні IoT-пристрої. І по-третє, EM-SCA застосовний лише тоді, коли пристрій працює під час огляду. Якщо пристрій вимкнений і не виконує жодних операцій, провести аналіз у цьому випадку неможливо.

Який найсильніший висновок цієї роботи?

Найсильніший висновок полягає в тому, що електромагнітний побічний канал можна переосмислити. Замість суто наступальної парадигми – викрадення ключів, шпигунство – він може стати неінвазивним криміналістичним сенсором, що дає змогу зазирнути у внутрішню поведінку IoT-пристрою навіть тоді, коли класичне вилучення даних недоступне. Це не просто технічний трюк, а потенційно новий напрям цифрової криміналістики.

Чому це важливо вже сьогодні

IoT-пристрої дедалі глибше вростають у реальний світ: вони вимірюють, слухають, показують, відчиняють, записують і супроводжують повсякденні дії людей. Але саме ця

повсюдність робить їх особливо складними для слідства. Дисертація показує, що у майбутньому слідчий може працювати не лише з файлами, журналами та образами пам'яті, а й із хвилями – з електромагнітними відбитками роботи пристрою. І це, можливо, один із найцікавіших зсувів у всій логіці цифрового доказування.

Фінальний висновок

Ми звикли вважати, що цифровий доказ – це те, що десь записано. Ця робота пропонує іншу, значно ширшу картину: доказом може бути і те, як пристрій поводиться в момент своєї роботи, і який електромагнітний слід він при цьому залишає. Дисертація Electromagnetic Side-Channel Analysis Methods for Digital Forensics on Internet of Things показує, що майбутнє криміналістики лежить не лише в пам'яті пристроїв, а й у фізиці їхнього функціонування. І чим більше світ наповнюється IoT-системами, тим важливішим стає вміння читати не лише дані, а й хвилі.

Як оптичні побічні випромінювання повернули стару TEMPEST-проблему в нову цифрову епоху [4]

Ми звикли сприймати індикаторні світлодіоди як найневиннішу частину електроніки. Вони просто блимають, показують активність, сигналізують про стан лінії чи пристрою. Але саме в цій простоті й ховається пастка. Стаття Optical TEMPEST нагадує про те, що світло теж може бути побічним каналом витоку. Іноді достатньо швидкий LED, який людське око бачить як стабільно увімкнений, насправді передає значно більше – іноді навіть зміст даних. Ця робота не просто згадує ранні дослідження оптичного TEMPEST, а показує, як стара вразливість повертається в нових технологічних умовах: з IoT, дронами та вимогами приватності.

Що таке optical TEMPEST, якщо пояснити дуже просто?

Це витік інформації через світлові випромінювання електронних пристроїв. Якщо індикатор, екран або інше оптичне джерело змінює яскравість відповідно до внутрішніх цифрових процесів, то сторонній спостерігач із достатньо швидким фотодетектором може спробувати відновити корисну інформацію. Ідеться не про те, що людина помітить миготіння очима, а про те, що прилад побачить часову структуру світла, яка неочевидна для людини.

Тобто звичайний світлодіод на корпусі може бути джерелом витоку?

Саме так. У ранніх дослідженнях було показано, що частина LED-індикаторів реагує достатньо швидко, щоб відтворювати високошвидкісні цифрові сигнали. Для людини світлодіод, що мерехтить швидше приблизно 30 Гц, виглядає просто постійно ввімкненим. Але для фотодетектора це вже носій інформації. У статті прямо зазначено, що LED дешеві, надійні й дуже швидкі, а тому привабливі для розробників і водночас небезпечні з погляду інформаційної безпеки.

З чого взагалі почалася ця історія?

Автор описує майже детективний початок. У 1992 році, працюючи в банку в Сіетлі, він помітив підозрілу поведінку індикаторів у комп'ютерному середовищі, заповненому модемами, Ethernet-обладнанням і лініями зв'язку. Подальші обережні експерименти показали, що деякі оптичні сигнали справді корелюють із тим, що обробляє пристрій. Так і було відкрито те, що згодом дістало назву optical TEMPEST.

І що саме тоді вдалося встановити?

У ранній роботі всі пристрої було поділено на три класи ризику. Клас I показував лише стан пристрою, клас II – рівень активності, а клас III – уже самі дані, тобто зміст інформації. Саме клас III є найбільш небезпечним, і в підсумковій таблиці статті зазначено, що близько 36% протестованих тоді пристроїв належали саме до цього класу. Це означало, що більше третини зразків давали витік не просто ознакам роботи, а інформаційному змісту.

Які пристрої виявилися найнебезпечнішими?

Переважно пристрої передавання даних. У статті сказано, що оптичні випромінювання III класу майже повністю спостерігалися саме в комунікаційному обладнанні – від дешевого до дуже дорогого. Особливо небезпечними були індикатори, підключені безпосередньо до ліній передачі даних, без буферизації або спеціального "розтягування" імпульсів під потреби людського ока.

Але ж сьогодні Ethernet-обладнання виглядає менш вразливим. Чому?

Це один із найцікавіших висновків статті. Автор пояснює, що масове зниження ризику в Ethernet стало наслідком поділу на MAC і PHY. У стандартному Ethernet фізичний рівень реалізується спеціалізованими PHY-чипами, які мають окремі виводи для LED-індикаторів і всередині самі "розтягують" короткі імпульси, щоб активність була видима людині, але не повторювала сирий високошвидкісний потік даних. Тобто стандартизація та правильний дизайн ланцюга індикації фактично зменшили вразливість мільярдів пристроїв.

Тобто проблема була не в самому LED, а в тому, як його під'єднали?

Саме так. Світлодіод сам по собі просто швидкий. Небезпека виникає тоді, коли розробник напряму "садить" його на сигнал, який несе дані. У статті це описано дуже виразно: спокуса для інженера зробити дешево, просто й надійно була надто великою, тому індикатор нерідко фактично ставав оптичним репітером цифрової активності. А звичайні LED здатні добре відтворювати амплітудно-модульовані сигнали аж до наносекундних масштабів без жодних спеціальних драйверів.

У статті є цікавий мотив "втрачених можливостей". Про що йдеться?

Автор відверто розповідає про власну помилку. Він колись відкинув ідею шукати оптичні побічні випромінювання у відеодисплеїв, бо вважав це фізично малоймовірним. А тим часом Маркус Кун подивився – і знайшов. Це важлива наукова мораль цієї статті: іноді вразливість існує саме там, де її вважають неможливою ще до експерименту. У цій історії той, хто подивився, виявив те, що інший пропустив.

Чому автор називає цю тему знову актуальною сьогодні?

Тому що старі уроки безпеки мають властивість забуватися. У вступі автор прямо пише, що нові технологічні тенденції – IoT, високочастотна торгівля, вимоги приватності на кшталт GDPR, дешеві дрони – повернули актуальність цієї проблеми. Загальний принцип безпеки, який проходить через усю статтю, звучить просто: вразливості, навіть виправлені, іноді не залишаються виправленими назавжди.

А де тут з'являється високочастотна торгівля? Це ж зовсім інший світ.

Саме цим і цікава стаття. Автор припускає, що в системах високочастотної торгівлі інженери,

женучись за мікросекундами затримки, могли викидати або спрощувати захисні елементи, які у звичайному Ethernet-дизайні вже давно стали нормою. Якщо в bespoke FPGA або ASIC-рішеннях індикатори чи діагностичні LED підключені необережно, вони потенційно можуть відкрити "вікно" для оптичного спостереження. Це в статті прямо подано як попередження про небезпеку "ковбойської інженерії", коли оптимізація швидкості стирає неочевидні бар'єри безпеки.

Я бачу, що друга половина статті переходить від аналізу вразливості до проєктування захищеного продукту. Чому такий поворот?

Бо ця стаття – не лише ретроспектива, а й практичний урок про те, як будувати нові пристрої після засвоєння помилок. Автор описує проєктування нового безпекового продукту з урахуванням принципів optical TEMPEST, зокрема для задач приватності в медичному середовищі. Там ідеться не про те, як "виловити" черговий витік, а про те, як одразу закласти в архітектуру фізичні бар'єри, які не дозволять витоку виникнути.

Які головні принципи такого захищеного дизайну?

Простота і прозорість реалізації. Автор підкреслює, що довіряти слід не складності, а мінімалізму: менше компонентів, менше прихованих функцій, менше закритих IP-блоків, більше можливості перевірити все руками і очима. У прикладі з фотодіодним приймачем наголошено, що схема зроблена максимально простою не заради економії деталей, а заради прозорості оцінювання безпеки. Далі ця ж логіка переноситься на весь пристрій.

У статті є сильний термін – "energy gap". Що він означає?

Це розширення звичного поняття "air gap". Автор посилається на ідею, що просто фізично відокремити систему вже недостатньо, бо інформація може просочуватися через різні фізичні канали: радіочастотні, акустичні, оптичні, теплові, магнітні

тощо. Тому потрібен не просто повітряний розрив, а енергетичний розрив – тобто така архітектура, де фізичні механізми перешкоджають витоку енергії як носія інформації. У його проєкті це досягається оптичними, механічними й фізичними бар'єрами між доменами.

Який головний урок для сучасних інженерів?

Те, що безпеку не можна зводити до "очевидного". Дуже простий, дешевий, надійний індикатор може виявитися каналом витоку. Дуже розумна оптимізація може зруйнувати старі, непомітні, але важливі захисні властивості стандартного дизайну. І головне – технічний прогрес постійно змінює межу можливого для атаки: те, що вчора було малоймовірним, завтра може стати доступним завдяки кращим датчикам, дешевшим дронам або новим сценаріям спостереження.

Чому це важливо вже сьогодні

Optical TEMPEST змушує по-новому подивитися на саму ідею "безпечного" індикатора. У світі, де електроніка дедалі частіше працює в режимі повної прозорості – мережі, сенсори, медичні системи, пристрої IoT – навіть світло стає носієм ризику. І що більше покладаються на швидкість, мініатюризацію та дешеві компоненти, то вищий шанс, що десь у проєкті знову з'явиться забутий старий канал витоку. Стаття фактично попереджає: проблема не зникла, вона просто змінює форми разом із технікою.

Фінальний висновок

Optical TEMPEST – це нагадування про одну з найнеприємніших істин безпеки: інформація витікає не лише через мережу, пам'ять або помилки в коді, а й через саму фізику пристрою. Світлодіод, задуманий як зручний засіб індикації, може стати мовчазним передавачем даних. І саме тому справжня безпека починається не там, де ми додаємо ще один захисний механізм, а там, де ми ставимо собі незручне запитання: чи не говорить наш пристрій назовні більше, ніж ми йому дозволили?

Як нелінійне розсіяння в оптичному волокні дозволяє знаходити підслуховувача з точністю до сантиметрів [5]

У сучасних волоконно-оптичних мережах загроза перехоплення давно перестала бути суто теоретичною. Ми звикли думати про захист каналу в термінах шифрування, квантового розподілу ключів і математичної стійкості протоколів. Але навіть коли система вміє виявити аномалію, залишається болюче практичне питання: де саме сидить порушник? Стаття Eavesdropper localization for quantum and classical channels via nonlinear scattering пропонує відповідь, яка звучить майже як технічна інтуїція майбутнього: шукати зловмисника не за грубими втратами в лінії, а за дуже локальними змінами акусто-оптичної взаємодії у волокні. І робити це з точністю до сантиметрів.

У чому головна ідея вашої роботи?

Ми досліджували, як після виявлення атаки локалізувати потенційного підслуховувача в оптичному каналі – як у квантовому, так і в класичному. Основна ідея полягає в використанні стимульованого розсіяння Бріллюена та Brillouin optical correlation domain analysis (BOCDA) для дуже точного просторового картографування волокна. Це дозволяє не просто сказати, що канал скомпрометовано, а вказати місце втручання з сантиметровою точністю.

Чому для цього недостатньо звичайних методів моніторингу волокна?

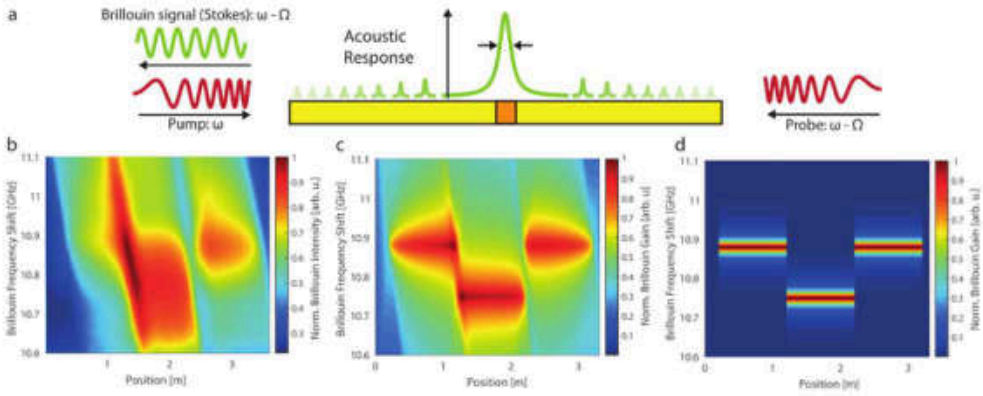
Бо типові методи, зокрема OTDR, добре бачать грубі порушення – розриви, торці, великі відбиття, різкі неоднорідності. Але реалістична атака на волоконний канал часто виглядає набагато делікатніше. Наприклад, це може бути еванесцентний відбір через вигин волокна або відгалужувач із малим коефіцієнтом відбору. Такі втручання не створюють різкої "неоднорідності" в лінії, тому класичні підходи швидко впираються в межі чутливості. Саме в цій зоні і починає працювати наш підхід.

Чому ця проблема особливо важлива для QKD?

Тому що квантовий розподіл ключів може виявити факт втручання, але цього замало для практичної стійкості системи. Якщо канал позначено як небезпечний, генерація ключа може зупинитися. Це відкриває шлях до denial-of-service: зловмисник не обов'язково має непомітно красти інформацію – йому достатньо зірвати роботу системи. Щоб відновити нормальну роботу, потрібно швидко знайти й усунути джерело втручання. Саме тому локалізація підслуховувача стає не додатковою функцією, а елементом життєздатності каналу. Після зупинки квантового обміну система локалізації вмикається й сканує волокно між абонентами.

Як працює ваш метод у фізичному сенсі?

Ми використовуємо прямо частотно-модульовану BOCDA-схему. У волокно з двох боків вводяться pump і probe хвилі, частотно узгоджені так, щоб у певній локальній ділянці виникала стимульована акустична відповідь. Через корельовану модуляцію ця взаємодія "замикається" лише в конкретній позиції волокна. Саме ця позиційна локалізація дає змогу знімати Brillouin-відгук не вздовж усього каналу одразу, а майже точково, з дуже малою просторовою протяжністю. У результаті ми отримуємо не просто інтегральну характеристику лінії, а просторово розділену карту Brillouin-спектра.



a) Схема прямочастотно-модульованого оптичного кореляційного доменного аналізу Бріллюена (BOCDA) в оптичному хвилеводі.
b) Типове вимірювання BOCDA оптичного волокна 980A (позиція 1,1 – 2,1 м), вбудованого всередині двох волокон SMF28 (позиції 0,1 – 1,1 м та 2,1 – 3,1 м). Зсув частоти Бріллюена (BFS) показано залежно від положення вимірювання.
c) Повне моделювання вимірювання BOCDA в частотній області.
d) Отриманий спектр посилення без фону, що виникає внаслідок частотних кореляцій.

Наскільки точним є такий підхід?

У наших експериментальних параметрах ми досягли просторової роздільної здатності 3,0 см. Це прямо випливає з обраної смуги модуляції та частоти модуляції в BOCDA. При цьому відстань між кореляційними точками можна збільшувати до кілометрів, зменшуючи частоту модуляції. Саме ця комбінація – сантиметрова локалізація плюс робота на довгих каналах – і робить метод особливо привабливим для мережевої безпеки.

Який тип атаки ви моделювали як найреалістичніший?

Ми зосередилися на еванесцентному відборі через вигин волокна. Це дуже показовий випадок, бо він дає зловмиснику доступ до частини сигналу, але не створює грубого пошкодження лінії. Ми досліджували втрати на рівні 1%, 5% і 10% від повної передачі. І показали, що навіть при 1% outcoupling можна чітко локалізувати ділянку втручання завдяки локальній зміні інтенсивності Brillouin-взаємодії.

Чому ви вважаєте результат для 1% особливо важливим?

Тому що 1% – це вже дуже "акуратне" втручання. Воно не виглядає як груба аварія, і саме тому має практичний сенс для атаки. Якщо система здатна впевнено локалізувати настільки слабкий евенесцентний відбір, це означає, що вона працює не лише на великих катастрофічних подіях, а й на тонких, малопомітних спробах підслуховування. У статті ми прямо наголошуємо, що саме тут сантиметрова просторова роздільність дає вирішальну перевагу.

Ви розглядали лише вигин волокна?

Ні. Ми також протестували комерційно доступні оптоволоконні оптичні відгалужувачі і показали, що навіть для показника відгалуження в 1% можна чітко локалізувати точку відбору. Цікаво, що в цьому

випадку корисною виявляється вже не лише інтенсивність Brillouin-сигналу, а й зміна максимального Brillouin frequency shift (BFS).

Один із найбільш незвичних результатів у статті – це "відбитки" стандартного SMF28. Що саме ви показали?

Ми виявили, що навіть стандартні одномодові волокна SMF28 від різних виробників мають досить відмінний Brillouin сигнатуру. Їхній максимум BFS розрізнявся на кілька мегагерц. Це дозволило нам чітко відрізняти волокна Thorlabs, Opneti та Newport, а також ідентифікувати навіть 6-сантиметрову вставку чужого SMF28, зварену всередину іншого сегмента. Це дуже важливо: виходить, що навіть зовні однакове стандартне волокно може нести акусто-оптичний "підпис" свого походження.

Чому цей результат такий сильний з точки зору безпеки?

Тому що він відкриває дорогу до волоконної атрибуції. Якщо під час технічного обслуговування, ремонту чи несанкціонованого втручання в канал хтось додасть новий сегмент волокна, його можна буде виявити не лише як "якийсь дефект", а як чужорідну вставку з іншим акусто-оптичним профілем. Для високозахищених середовищ це означає можливість не просто стежити за каналом, а буквально "пам'ятати", з чого він складається. У статті автори навіть прямо говорять про перспективу спеціально підібраних або "відфінгерпринтованих" волокон для середовищ із високими вимогами до безпеки.

І все це ви порівняли зі звичайним OTDR?

Так, і це був важливий тест реальності. Ми використали комерційний високороздільний Rayleigh OTDR із 2 нс імпульсами та 2,5 см sampling resolution. Але він не зміг відтворити наші результати. Зокрема, не вдалося впевнено побачити ні вигин із втратами до 10%, ні відмінності між SMF28 від різних виробників, ні коротку гібридну вставку, ні положення слабких splitter-ів.

Тобто ваш підхід перемагає OTDR саме там, де втручання плавне, а не різке?

Саме так. OTDR сильний у пошуку дискретних відбиттів і грубих неоднорідностей. Натомість наш метод добре бачить поступові зміни показника заломлення і локальні зміни в нелінійній акусто-оптичній взаємодії. А саме так часто і виглядають реальні техніки підслуховування: вони не рвуть канал, а дуже обережно знімають частину енергії. Це ключова перевага Brillouin correlation-domain підходу.

Наскільки цей метод придатний для реального впровадження?

Ми вважаємо, що він може працювати як окремий засіб моніторингу, але особливо перспективним є його вбудовування в QKD-системи, наприклад у режимі перемикання. Тобто система може періодично або за тригером переходити з режиму квантового обміну в режим локалізаційного сканування каналу. Це дає не просто реакцію на атаку, а постійне картографування довіреного стану встановленої мережі. У висновку ми прямо зазначаємо, що це відкриває шлях до систематичного моніторингу встановлених ліній в реальному часі.

Який головний висновок із вашої роботи?

Що фізичний рівень безпеки волоконного каналу можна підняти на новий рівень. Ми показали метод, який уміє локалізувати дуже слабкі втручання з сантиметровою точністю, розпізнавати чужорідні волоконні сегменти і робити це однаково релевантно для квантових і класичних каналів. Це означає, що захист каналу перестає бути лише питанням криптографії й переходить у режим точної фізичної інспекції самої лінії.

Чому це важливо вже зараз

У безпеці оптичних мереж довгий час панувала майже мовчазна домовленість: якщо немає великого розриву або грубої втрати, то канал, мабуть, “цілий”. Ця стаття руйнує таке припущення. Вона показує, що реальна загроза може бути

малою, акуратною і майже невидимою для традиційних інструментів. І що саме в таких випадках нелінійна фізика волокна – через Brillouin-розсіяння – може стати не академічною екзотикою, а новим інструментом технічного захисту мереж.

Фінальний висновок

Оптичне волокно давно стало символом швидкості, дальності та пропускної здатності. Але в цій роботі воно постає ще й як сенсор власної цілісності. Стаття Eavesdropper localization for quantum and classical channels via nonlinear scattering показує, що майбутнє захищених комунікацій залежить не лише від того, наскільки добре ми шифруємо повідомлення, а й від того, наскільки точно вміємо діагностувати сам канал. І, можливо, найцікавіше тут те, що підслуховувача в оптичній мережі тепер можна шукати не лише логікою протоколів, а й фізикою звуку, який народжується всередині світла.

Як гнучка п'єзоелектрична структура перетворюється на активний бар'єр проти витоку мовної інформації через вібрації [6]

Ми звикли думати, що розмова зникає в повітрі, щойно замовкають голоси. Але для сучасних засобів акустичного шпигунства цього давно недостатньо. Мова залишає слід не лише в повітряному середовищі, а й у мікровібраціях предметів: столів, скла, стін, труб, панелей. Саме ці слабкі механічні коливання можуть стати носієм конфіденційної інформації. Стаття Research on Active Interference Technology Based on Piezoelectric Flexible Structure пропонує практичну відповідь на цю загрозу: не просто ізолювати приміщення, а активно нав'язувати поверхні власну вібрацію, яка перекриває корисний мовний слід. І робити це за допомогою гнучкої, переносної, швидко розгортуваної п'єзоелектричної структури.

У чому головна ідея вашої роботи?

Ми розробили piezoelectric flexible interference structure (PFIS) – гнучку п'єзоелектричну структуру для активного вібраційного маскування. Її мета – створення завадити відновленню мовної інформації з мікровібрацій поверхонь, які виникають під дією людського голосу. Інакше кажучи, ми не просто глушимо звук у повітрі, а навмисно змушуємо саму поверхню вібрувати сильніше й "неправильно" з точки зору підслуховувача.

Чому сьогодні це важливо?

Тому що сучасне акустичне підслуховування дедалі частіше працює не напряму зі звуком, а через вібраційні на об'єктах. У статті прямо зазначено, що відновлення мовлення може виконуватися через датчики, оптичні засоби або радіочастотні методи, які знімають дуже слабкі коливання поверхні. Типовий приклад – лазерне підслуховування через віконне скло або поверхню стола. Якщо поверхня коливається під дією мовлення, її можна використати як непрямий носій інформації.

Чим ваш підхід відрізняється від звичайного пасивного захисту?

Пасивний захист зазвичай означає потовщення конструкцій, зміну матеріалів, багатошарові вікна, покриття, переробку будівельних елементів. Такі методи можуть працювати, але вони складні, ресурсомісткі й погано підходять для тимчасових або швидко розгортуваних приміщень. Ми орієнтувалися саме на сценарії, де потрібне швидке розгортання. Тому запропонували активний підхід: переносний пристрій кладеться на поверхню й одразу створює маскувальні вібрації без клею, стаціонарного монтажу чи перебудови приміщення.

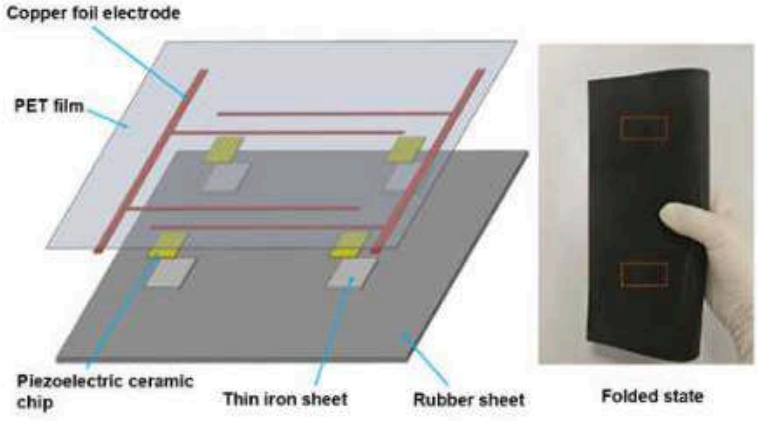
Чому ви обрали саме п'єзоелектричну структуру?

Бо традиційні збудники вібрації мають обмеження. Звичайні exciters часто гірше працюють на високих частотах, а електромагнітні актуатори бувають занадто великими. П'єзоелектричні матеріали, навпаки, мають малу масу, широкий частотний діапазон, прості в інтеграції й добре підходять для компактних активних систем. Ми використали ці переваги, але подали їх у формі гнучкої переносної конструкції, а не жорстко вбудованого вузла.

Як виглядає PFIS конструктивно?

Структура складається з кількох шарів: гумова основа, тонкий залізний лист, п'єзокерамічна пластина, мідний електрод і захисна PET-плівка. Гумова основа забезпечує гнучкість, тож PFIS можна згинати або складати під час транспортування. Металева пластина компенсує крихкість кераміки. PET-плівка виконує захисну функцію. У статті наведено також геометричні параметри всіх елементів і схема конструкції.

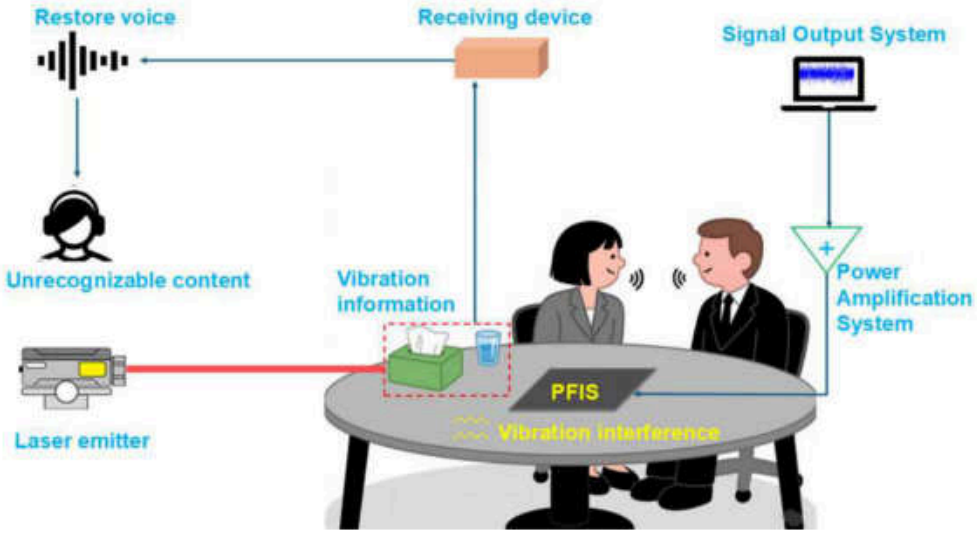
Конструкція структури п'єзоелектричного актуатора та його вид у складеному стані



Ви наголошуєте на швидкому розгортанні. Що це означає на практиці?

Це означає, що PFIS не потрібно приклеювати до поверхні. Його просто кладуть на стіл, підлогу або іншу відносно плоску конструкцію. Він працює через контактну передачу вібрації. Це спрощує використання в тимчасових переговорних, мобільних штабах, швидко обладнаних кімнатах для нарад – там, де часу на монтаж практично немає.

Принцип роботи використання PFIS для активного вібраційного придушення для досягнення антилазерного прослуховування



Але якщо він просто лежить на поверхні, чи не втрачається ефективність передачі вібрації?

Саме тому ми окремо досліджували вплив додаткового навантаження. Коли PFIS просто лежить на поверхні, контактний тиск нижчий, а отже нижча й ефективність передавання механічної енергії. Коли ж зверху додається маса, контакт стає щільнішим, площа притискання збільшується, а передача вібрації покращується. Це один із ключових практичних результатів статті.

Які саме сигнали ви використовували для маскування?

Ми перевірили три типи сигналів: білий шум, звук вітру в листі і барабанний ритм. Ідея була в тому, щоб оцінити не лише "силу" маскування, а й практичну придатність. Білий шум показує найвищу вібраційну потужність, але природні звуки чи музичні сигнали

можуть бути комфортнішими для людей у приміщенні. Тобто в статті розглядається не тільки технічна ефективність, а й баланс між захистом і комфортом.

Який результат давали ці сигнали без додаткової ваги?

Уже при 5 V peak-to-peak усі три сигнали створювали на поверхні стола вібрацію, що була значно сильнішою, ніж від самого людського голосу. Для білого шуму середня вібраційна відповідь становила 0.1668 м/с², для шуму листя – 0.0468 м/с², для барабанів – 0.0240 м/с². Для порівняння, при одному лише голосі середня відповідь стола була 0.0172 м/с². Тобто навіть без додаткових хитрощів структура вже створювала домінуючу вібраційну заваду.

А що відбувається, коли підвищувати напругу?

У роботі показано майже лінійний ефект: що вища напруга, то сильніша вібраційна відповідь. Зі зростанням напруги від 5 до 30 V зростають і середні, і максимальні значення прискорення на поверхні. Тобто керування напругою – це прямий інструмент регулювання сили маскування. Автори окремо підкреслюють, що збільшення напруги покращує інтерференційну дію в усьому частотному діапазоні.

А який ефект дає додаткова вага?

Дуже помітний. Коли зверху на PFIS додавали масу до 3.5 кг, загальна вібраційна ефективність значно зростала. У статті прямо сказано, що при 3.5 кг вібраційна продуктивність PFIS підвищувалася приблизно в 5.6 раза порівняно з випадком без додаткової ваги. При цьому до приблизно 1 кг залежність була майже лінійною, а далі приріст поступово насичувався.

Чи однаково добре працює така система на всіх частотах?

Ні, і це один із важливих нюансів статті. Автори показали, що після 2500 Гц додавання ваги суттєво

покращує вібраційну заваду. Нижче 2500 Гц ефект від ваги значно слабший. Натомість підвищення напруги покращує інтерференцію в усьому діапазоні, включно з нижчими частотами. Це означає, що для подальшої оптимізації PFIS потрібно окремо працювати з низькочастотною зоною, наприклад адаптивно керувати амплітудою різних частотних компонентів.

А як ви оцінювали, чи справді мовлення стало нечітким для відновлення?

Ми не обмежувалися лише механічними вимірюваннями. У роботі виконано ще й аналіз спектрограм відновленого мовлення, отриманого з вібрацій поверхні. Без завади мовний "voiceprint" у спектрограмі був добре видимий, і зміст мовлення можна було розрізнити. При білому шумі та 5 V більша частина цього відбитка вже маскувалася, але в діапазоні 0–2500 Гц ще залишалися фрагменти. При 30 V голосовий відбиток був майже повністю перекритий.

Тобто ваш підхід працює не лише "по приладах", а й по змісту?

Саме так. Автори окремо підкреслюють, що відновлений із вібрацій голос при наявності сильного білого шуму від PFIS стає нерозпізнаваним за змістом. Це принципово важливо: мета не в тому, щоб просто збільшити прискорення на поверхні, а в тому, щоб зруйнувати можливість коректного відновлення мовної інформації.

Які слабкі місця або обмеження ви самі бачите в цій технології?

У статті їх названо прямо. По-перше, додаткова вага покращує роботу, але зменшує зручність транспортування. Самі автори пропонують у майбутньому замінити її, наприклад, надувними повітряними камерами, які створювали б тиск без масивного вантажу. По-друге, ефективність PFIS залежить від характеристик поверхні – шорсткості, жорсткості, контактних умов. У роботі випробування проводилися на дерев'яній стільниці, але для інших поверхонь потрібні окремі дослідження.

Який головний висновок із вашої роботи?

Що активне вібраційне маскування можна зробити переносним, швидко розгортуваним і практично ефективним. PFIS показала, що п'єзоелектрична гнучка структура здатна створювати заваду, яка перекриває вібрації від людського голосу і робить відновлене мовлення непридатним для розпізнавання. А це означає, що для захисту конфіденційних переговорів тепер можна працювати не лише з повітряним шумом, а й безпосередньо з механікою поверхні.

Чому це важливо вже зараз

Найцікавіше в цій роботі те, що вона зміщує саму логіку захисту. Раніше ми переважно боролися з підслуховуванням або через послаблення джерела, або через ізоляцію простору. Тут підхід інший: поверхня, яка могла б стати "свідком" розмови, примусово перетворюється на джерело контрольованого хаосу. І це особливо цінно для тимчасових або мобільних середовищ, де неможливо перебудувати стіни, змінити скло чи монтувати складні стаціонарні системи.

Фінальний висновок

Стаття Research on Active Interference Technology Based on Piezoelectric Flexible Structure показує просту, але сильну річ: у боротьбі за захист мовної інформації важливо не лише приховати голос, а й зірвати роботу тих фізичних носіїв, через які він може бути відновлений. PFIS робить саме це – перетворює звичайну поверхню з пасивного переносника мовлення на активне поле завади. І, можливо, саме в такому підході – легкому, гнучкому, контактному й швидко розгортуваному – формується нове покоління практичного захисту від вібраційного акустичного шпигунства.

Як технічні канали витоку через побічні електромагнітні випромінювання змушують по-новому дивитися на захист інформації [7]

У розмовах про інформаційну безпеку часто домінують шифрування, мережеві атаки, контроль доступу й програмні вразливості. Але є інший, значно старіший і фізично реальніший рівень загрози: інформація може залишати систему не через помилку в коді, а через сам принцип роботи технічних засобів. Коли електроніка передає, обробляє або зберігає дані, вона неминуче породжує супутні електромагнітні, електричні, акустичні й оптичні прояви. Саме вони й стають основою технічних каналів витоку. Стаття Methods and techniques of protecting information from leakage by technical channels via side electromagnetic radiation цікава тим, що не зосереджується на одній екзотичній атаці, а намагається систематизувати весь ландшафт таких загроз і показати, як будувати захист – від пошуку закладних пристроїв до екранування, фільтрації, заземлення та активного зашумлення.

У чому головна ідея вашої статті?

Ми прагнули систематизувати технічні канали витоку інформації, що виникають через побічні електромагнітні випромінювання та інші фізичні прояви роботи технічних засобів, а також узагальнити методи їхнього виявлення й захисту. У статті наголошується, що проблема витоку через технічні канали загострюється разом із розвитком комп'ютерної техніки, бездротових систем, персональної електроніки та зростанням функціональності сучасних електронних засобів.

Що ви називаєте технічним каналом витоку інформації?

Це неконтрольоване поширення інформативного сигналу від джерела через фізичне середовище до технічного засобу, здатного цей сигнал виявити, прийняти й обробити. Інакше кажучи, йдеться про ситуацію, коли сама фізика роботи системи створює побічний шлях для перехоплення інформації. У статті підкреслюється, що особливості таких каналів визначаються природою інформаційного сигналу і характеристиками середовища поширення.

Які типи технічних каналів витоку ви виділяєте?

У роботі подано загальну класифікацію, яка включає чотири великі групи: канали витоку під час оброблення інформації технічними засобами, технічні канали витоку мовної інформації, канали витоку під час передавання інформації каналами зв'язку та канали витоку візуальної інформації.

Якщо говорити саме про технічні засоби оброблення інформації, які канали ви вважаєте найважливішими?

Для технічних засобів оброблення інформації виділяються три головні групи: електромагнітні, електричні та параметричні канали. До електромагнітних належать побічні електромагнітні випромінювання й наведення, випромінювання на робочих частотах генераторів, а також на частотах самозбудження підсилювачів. До електричних – витік інформаційних сигналів у лініях живлення, у контурах заземлення та витік через закладні пристрої. Параметричні канали пов'язані з перехопленням інформації шляхом високочастотного опромінення технічних засобів.

Тобто класичний TEMPEST тут лише одна частина ширшої проблеми?

Саме так. Хоча побічні електромагнітні випромінювання і наведення є центральною темою, стаття демонструє, що технічний витік – це ширше поняття. Поруч із SEMRG розглядаються витоки через акустичні й віброакустичні канали, через оптичне спостереження, через комунікаційні лінії та навіть через фізичні параметри елементів системи. Тобто TEMPEST тут не ізольована аномалія, а частина загальної фізичної моделі інформаційного витоку.

У статті багато уваги приділено закладним пристроям. Чому?

Тому що вони є практичним засобом експлуатації технічних каналів витоку. Автори окремо описують закладні пристрої, які можуть перехоплювати інформацію з монітора, клавіатури, периферійних

пристроїв або носіїв даних. При цьому перехоплена інформація або одразу передається радіоканалом, або записується на проміжний носій, а потім передається за командою. Інакше кажучи, побічний канал сам по собі ще не є повною атакою – але закладний пристрій робить його інструментом практичного шпигунства.

Які засоби пошуку таких пристроїв розглядаються у вашій роботі?

Досить широкий спектр. У статті згадуються візуальний огляд, детектори диктофонів і відеокамер, індикатори поля, радіочастотоміри, інтерсептори, сканувальні приймачі, спектроаналізатори, програмно-апаратні комплекси контролю, нелінійні локатори, рентгенівські системи, а також прилади для перевірки провідних ліній. Вибір методу суттєво залежить від типу засобу контролю та характеру очікуваного закладного пристрою.

Чому, наприклад, нелінійні локатори вважаються такими важливими?

Тому що вони реагують на нелінійні властивості напівпровідникових елементів. Це дозволяє знаходити електронні компоненти закладних пристроїв навіть тоді, коли ті добре замасковані. У статті прямо сказано, що серед засобів виявлення саме нелінійні радари дають одні з найнадійніших результатів, оскільки приймають другу й третю гармоніки відбитого сигналу, що виникають через нелінійність характеристик напівпровідників.

Як ви описуєте витік під час передавання інформації каналами зв'язку?

Тут стаття наголошує, що практично будь-який канал зв'язку за відсутності належного криптографічного захисту може стати природним каналом витоку. Згадуються короткохвильові, ультракороткохвильові, радіорелейні, тропосферні, супутникові, стільникові, кабельні та волоконно-оптичні лінії. Для них виокремлюються електромагнітні, електричні та індукційні способи перехоплення. Особливо цікаво, що для волоконно-оптичних ліній автори окремо

описують фізичні причини оптичних втрат і можливого витоку – зміщення стиків, зазори, кутову невідповідність, різницю діаметрів волокон, вигини та пошкодження. У статті є й розділ про мовну інформацію.

Які канали витоку вважаються основними?

Розглядаються п'ять груп: прямі акустичні канали, віброакустичні, акусто-оптичні (лазерні), акусто-електричні та акусто-електромагнітні. Прямі акустичні канали спираються на поширення звуку в повітрі, віброакустичні – на коливання будівельних конструкцій, лазерні – на дистанційне зняття мікровібрацій із поверхонь, а електричні й електромагнітні – на перетворення акустичної інформації в електричні або електромагнітні сигнали. Таким чином, мовлення розглядається не просто як звук, а як явище, здатне залишати слід у різних фізичних середовищах.

А що з візуальною інформацією?

Тут автори нагадують, що витік може відбуватися через спостереження, зйомку об'єктів і копіювання документів. Для цього можуть використовуватися оптичні прилади, телекамери, далекофокусні системи, приховані відеокамери та портативні засоби фотографування. Цей розділ важливий тим, що показує: технічний витік – це не лише "радіо" чи "дроти", а будь-який фізичний спосіб перетворити інформаційний об'єкт на доступний для перехоплення сигнал або образ.

Які загальні принципи захисту ви вважаєте ключовими?

У статті наведено фундаментальні принципи технічного захисту: безперервність у просторі й часі, постійна готовність до нейтралізації загроз, багатозональність, вибірковість захисту для найбільш важливої інформації, інтеграція різних захисних систем. Окремо підкреслюється також надійність,

секретність, доцільність, різноманіття методів, комплексність і економічна обґрунтованість захисту. Це важливий момент: автори розглядають технічний захист не як окремий пристрій чи набір "засобів", а як повноцінну інженерну систему.

Якщо говорити саме про захист від SEMRG, які методи ви виділяєте?

Тут у статті проводиться класичний, але дуже корисний поділ на пасивні та активні методи. Їхня спільна мета – знизити співвідношення "сигнал/завада" на межі контрольованої зони до такого рівня, за якого небезпечний сигнал неможливо виділити засобами розвідки. Але роблять вони це по-різному: пасивні методи знижують рівень самого небезпечного сигналу, активні – підвищують рівень завад.

Що входить до пасивного захисту?

Насамперед це розділювальні трансформатори, фільтри придушення завад, екранування, заземлення і модернізація електронних пристроїв для зменшення рівня випромінювань. Автори пояснюють, що пасивний захист має послабити небезпечний сигнал до рівня, на якому його не можна виділити на тлі природних шумів. Це дуже інженерний підхід: не "заборонити витік", а фізично зробити його занадто слабким для корисного перехоплення.

А що входить до активного захисту?

Активний захист спрямований на створення просторових і лінійних маскувальних завад. У статті прямо сказано, що активні методи включають просторове та лінійне зашумлення. Це означає, що замість ослаблення джерела система навмисно формує середовище, в якому корисний сигнал губиться в завадах. Для акустичних і віброакустичних каналів такий підхід теж розглядається як один із центральних.

Чому екранування займає таке важливе місце у вашому викладі?

Тому що це базовий фізичний спосіб знизити електромагнітний витік. У статті окремо аналізуються електростатичне, магнітне, статичне й електромагнітне екранування, а також зазначено, що зі зростанням частоти практично ключовим стає саме електромагнітне екранування. Автори звертають увагу і на екранування приміщень, вікон, дверей, а також на спеціальні екрановані камери, які можуть забезпечувати ослаблення понад 100 дБ. Це вже не точковий захист, а повне керування електромагнітним середовищем об'єкта.

А як щодо заземлення? Чому ви приділяєте йому окрему увагу?

Бо без якісного заземлення екранування часто втрачає свою ефективність. У статті заземлення визначається як одна з найважливіших умов захисту від витоку через контури землі. Його завдання – відводити паразитні струми із екранів, корпусів та інших елементів і не дозволяти небезпечним потенціалам накопичуватися чи перекидатися на інші кола. Розглядаються одноточкові послідовні, одноточкові паралельні, багатоточкові та комбіновані схеми заземлення, показуючи, що тут теж немає універсального рішення: усе залежить від частотного режиму й архітектури системи.

Чому фільтрація та розділювальні трансформатори залишаються настільки актуальними?

Тому що значна частина небезпечних сигналів може поширюватися саме проводами живлення, заземлення чи інтерфейсними колами. У статті фільтрація названа одним із головних способів придушення провідних завад, а розділювальні трансформатори – засобом розв'язки первинних і вторинних кіл для недопущення наведень. Це дуже важливий висновок: TEMPEST-захист не закінчується на "екрані корпусу", бо сигнал може просто піти провідником далі.

Який головний висновок ви б хотіли, щоб читач виніс із цієї статті?

Що технічний витік інформації – це не сукупність окремих екзотичних загроз, а системна фізична проблема, яка потребує системного інженерного захисту. У висновку ми наголошуємо, що захист інформації від витоку технічними каналами через побічні електромагнітні випромінювання й наведення є важливим складником загальної системи інформаційної безпеки держави й суспільства. І що через постійну появу нових загроз методи й засоби захисту мають безперервно удосконалюватися.

Чому це важливо сьогодні

Цінність цієї статті не в тому, що вона пропонує одну "чарівну" технологію захисту. Її цінність у іншому: вона повертає розмову про безпеку на фізичний рівень. Сучасна інформаційна інфраструктура стає дедалі складнішою, але разом із цим не зникають, а лише множаться побічні прояви роботи систем – випромінювання, наведення, вібрації, оптичні сигнали, паразитні зв'язки. І чим більше таких проявів, тим важливіше формувати захист не лише через політики й програмні бар'єри, а через архітектуру середовища, конструкцію пристроїв і контроль фізичних каналів.

Фінальний висновок

Стаття Methods and techniques of protecting information from leakage by technical channels via side electromagnetic radiation нагадує про, можливо, найнеприємнішу правду технічного захисту: інформація починає витікати не тоді, коли хтось "зламав систему", а тоді, коли сама система в процесі своєї нормальної роботи породжує фізичні сліди, придатні для перехоплення. Саме тому справжній захист починається не з реакції на атаку, а з уміння бачити канал витоку ще до того, як ним скористалися. І в цьому сенсі стаття говорить не лише про SEMRG чи заземлення – вона говорить про культуру інженерного мислення, без якої інформаційна безпека завжди залишатиметься неповною.

Як мінімізація взаємної інформації перетворює штучний шум на точний інструмент протидії витоку побічними каналами [8]

У боротьбі з побічними каналами давно існує спокуса діяти грубо: якщо витік іде через споживання струму, часові коливання чи електромагнітні випромінювання, треба просто додати більше шуму. Але саме тут і виникає головна проблема сучасної вбудованої безпеки. Для серверів або потужних криптомодулів це ще може бути допустимим, а для IoT-пристроїв – уже ні. Там кожен міліват має вагу. Стаття Mutual Information Minimization for Side-Channel Attack Resistance via Optimal Noise Injection цікава тим, що ставить питання інакше: не як додати більше шуму, а як додати рівно стільки і саме туди де потрібно, щоб максимально зменшити витік інформації. І робить це через одну з найглибших ідей теорії інформації – мінімізацію взаємної інформації між секретом і побічними спостереженнями.

У чому головна ідея вашої роботи?

Ми розглядаємо побічний канал як канал зв'язку, через який атакувальник отримує інформацію про секрет. Якщо так, то природне завдання полягає в тому, щоб зменшити кількість інформації, яка проходить цим каналом. Саме тому ми формулюємо захист як задачу мінімізації взаємної інформації між секретною складовою і інформацією яку можна спостерігати в побічному каналі за умови обмеженої величини потужності на штучний шум.

Чому ви обрали саме взаємну інформацію як міру витоку?

Тому що вона безпосередньо відображає, скільки інформації про секрет можна винести зі спостережень. У статті ми пояснюємо це через нерівність Фано: якщо зменшити взаємну інформацію, зростає нижня межа ймовірності помилки атакувальника під час відновлення секрету. Інакше кажучи, менша взаємна інформація означає гіршу здатність супротивника правильно вгадати ключ або внутрішній стан.

Чим ваш підхід відрізняється від звичайного додавання шуму?

Більшість традиційних підходів або вводять шум рівномірно, або працюють евристично. Ми ж ставимо оптимізаційну задачу: маючи фіксований енергетичний бюджет, знайти такий розподіл штучного шуму між точками витоку, який мінімізує або сумарний, або максимальний витік інформації. Тобто ми не просто "заливаємо" систему шумом, а оптимально розподіляємо його там, де він реально дає найбільший захисний ефект.

Чому це особливо важливо для IoT-пристроїв?

Бо саме для них енергетична ціна контрзаходів є критичною. У статті прямо зазначено, що artificial noise injection вважається одним із найефективніших захисних засобів, але його великі енергоспоживчі показники роблять такий підхід проблемним для ресурсно-обмежених систем. IoT-пристрої часто не можуть дозволити собі "дорогі" захисні механізми, а значить їм потрібен не просто шум, а енергоефективний шум.

Як ви математично описуєте побічні канали?

Ми вводимо проміжний вектор X^m, який є функцією від секретної змінної U, а потім моделюємо спостереження як $Y^m=X^m+Z^m+N^m$, де Z^m – фізичний шум, а N^m – навмисно інжектований штучний шум. Далі кожну точку витоку можна трактувати як окремий підканал, і саме між ними ми розподіляємо потужність штучного шуму. Це дозволяє перейти від інтуїтивного захисту до формального інформаційно-теоретичного синтезу контрзаходу.

Ви розглядаєте два критерії оптимальності. Чому саме два?

Бо вони відповідають двом різним безпековим інтуїціям. Перша задача – мінімізувати сумарну або середню взаємну інформацію по всіх точках спостереження. Це середньостатистичний погляд на витік. Друга – мінімізувати максимальну взаємну

інформацію серед усіх точок. Це вже більш консервативний, "worst-case" підхід: якщо десь існує одна особливо небезпечна точка витоку, її потрібно придушити в першу чергу. Саме тому в статті розв'язуються обидві задачі.

З чого ви почали аналіз?

Спершу ми розглянули найзручніший випадок — коли вхідний сигнал має гаусівський розподіл, а канал є гаусівським. У такій ситуації взаємну інформацію можна записати у відомій формі, подібній до формули ємності гаусівського каналу. У статті з'являється дуже красивий образ подвійне "заповнення водою". Це означає, що оптимальний розподіл енергії має просту інтерпретацію: енергія розподіляється не довільно, а за певним пороговим правилом, подібним до класичного методу "заповнення водою", але в подвійній формі.

Що це означає?

У класичній теорії зв'язку "заповнення водою" – це спосіб оптимально розподілити потужність сигналу по паралельних каналах, щоб максимізувати сумарну пропускну здатність. У нас ситуація дзеркальна: ми розподіляємо потужність штучного шуму, щоб мінімізувати сумарний витік. Саме тому ми називаємо це подвійне "заповнення водою". Тобто ми не "наповнюємо" кращі канали корисним сигналом, а "заливаємо" небезпечні підканали шумом так, щоб зменшити їхню інформативність.

Що показало чисельне моделювання?

Для задачі мінімізації сумарної взаємної інформації запропонований метод стабільно досягає меншого середнього витоку. А для задачі мінімізації максимуму виграш ще помітніший: щоб зменшити піковий витік удвічі, наш підхід потребував на десятки відсотків менше шумової потужності, ніж рівномірне зашумлення.

А як щодо практичного сценарію з AES-128?

Ми виконали дослідження на реальних AES-128 із набору SPERO. Для цих трас сформували три режими захисту: рівномірне зашумлення, оптимальне зашумлення за критерієм сумарної взаємної інформації та оптимальне зашумлення за критерієм максимуму. Потім оцінили рівень успішного відновлення ключів при MIA-атаці. Обидва запропоновані методи перевершили рівномірний розподіл шуму, але особливо добре показав себе метод мінімізації максимальної взаємної інформації. У статті прямо наведено, що для досягнення рівня успіху 0.1 цей метод вимагав приблизно на 27.3% менше шумової потужності, ніж рівномірний розподіл.

Чому саме мінімізація максимуму дала кращий практичний результат?

Тому що в реальних реалізаціях витік часто локалізований. Не всі точки траси однаково небезпечні: є окремі операції, наприклад обчислення S-box, де інформативність значно вища. Якщо розподіляти шум рівномірно, значна частина енергії розподіляється на менш критичні ділянки. А коли ми цілеспрямовано спрямовуємо більше енергії на пікові діапазони частот витоку, то досягаємо кращого захисту за тієї ж потужності.

Який головний висновок із вашої роботи?

Що штучний шум має сенс лише тоді, коли він оптимально розподілений. Якщо просто додавати його всюди однаково, це дорого й не завжди ефективно. Якщо ж розглядати побічний канал як інформаційний канал і мінімізувати витік через взаємну інформацію, можна отримати захист, який є одночасно сильнішим і енергоощаднішим.

Чому це важливо вже зараз

Сьогодні захист інформації дедалі сильніше впирається не лише в криптографію, а в фізичну економіку пристрою. Для великих систем ще можна дозволити собі важкі контрзаходи, але майбутнє обчислень лежить у мільярдах малих пристроїв,

де захист повинен бути не просто ефективним, а оптимальним. У цьому сенсі стаття пропонує дуже сучасний підхід: безпека тут – це не надлишок шуму, а точна інформаційно-теоретична інженерія витоку.

Фінальний висновок

Стаття Mutual Information Minimization for Side-Channel Attack Resistance via Optimal Noise Injection показує, що шум у системі може бути не лише побічним небажаним явищем, а й ретельно спроєктованою формою захисту. Але лише за однієї умови: коли він вводиться не навмання, а з розумінням того, як саме інформація витікає назовні. І в цьому її головна сила – вона переводить захист інформації з рівня грубого маскування на рівень точного, математично оптимального керування витоком. Для світу IoT та енергообмежених систем це вже не просто красива теорія, а дуже практичний напрям майбутнього захисту.

Як відремонтований USB-кабель клавіатури відкриває несподіваний TEMPEST-канал витоку [9]

Ми звикли думати про ремонт кабелю як про повсякденну технічну дію: обрізати пошкоджену ділянку, з'єднати провідники, заізолювати – і пристрій знову працює. Але в електромагнітному світі така "дрібниця" може змінити все. Стаття Keystroke Detection by Exploiting Unintended RF Emission from Repaired USB Keyboards іііпоказує тривожний і дуже сучасний сюжет: традиційний ремонт кабелю USB-клавіатури здатен мимоволі створити маленьку монопольну антену, яка різко підсилює побічні RF-випромінювання. І якщо раніше такі витоки вважалися слабкими й локальними, то після ремонту їх уже можна використовувати для дистанційного виявлення натискань клавіш – навіть через 14-сантиметрову бетонну стіну й на відстанях до 12 метрів.

У чому головна ідея вашої роботи?

Ми досліджували, як звичайний ремонт пошкоджених кабелів впливає на електромагнітні побічні випромінювання. Головна ідея полягає в тому, що ремонт – зокрема скручування, пайка або використання butt-конекторів – може сформувати невелику монопольну антену. Вона підсилює ненавмисні електромагнітні випромінювання кабелю. У результаті слабкий електромагнітний побічний канал, який раніше був майже непрактичним, стає придатним для реальної атаки. У цій статті ми показали це на прикладі відновленого USB-кабелю клавіатури й продемонстрували дистанційне виявлення натискань клавіш.

Чому саме ремонт кабелю взагалі може створити антену?

Бо під час ремонту порушується первісна електромагнітна структура кабелю. Коли обірваний провідник скручують або паяють, виникає локальна неоднорідність, яка поводиться як короткий вертикальний випромінювач. У статті це прямо подано як мініатюрна монопольна антена. Вона неефективна в класичному антенному сенсі, але навіть цього достатньо, щоб значно підсилити випромінювання, які вже існували як побічний продукт передавання сигналу.

Чому це настільки небезпечно саме для USB-клавіатур?

Тому що сучасні USB-клавіатури до цього вважалися відносно менш вразливими за старі PS/2-клавіатури. У PS/2 був окремий тактовий сигнал, який створював сильніші випромінювання. У USB 2.0 ситуація інша: використовується диференційний протокол, а проводи DATA+ і DATA− скручені так, щоб зовнішні завади пригнічувалися, а побічні випромінювання двох протифазних сигналів частково компенсували одне одного. До того ж у кабелі є екранування. Саме тому звичайний USB 2.0-кабель дає значно менший витік. І саме тому результат ремонту виявився таким показовим: він фактично руйнує частину цієї природної електромагнітної "тиші".

Ви починали лише з клавіатур?

Ні. У попередній частині роботи ми перевіряли три типи кабелів: USB, силовий кабель і HDMI. У всіх випадках ремонтовані кабелі демонстрували сильніше випромінювання, ніж неремонтовані, і це випромінювання вдавалося виявити на відстані понад 4 м, а також через 14-сантиметрову бетонну стіну. Але в цій розширеній версії ми пішли далі й не просто зафіксували сам факт потужнішого електромагнітного сліду, а використали його для конкретної атаки – визначення натискань клавіш на USB-клавіатурі.

Чому ви обрали саме USB 2.0-клавіатуру як головну мішень?

Тому що це хороший контрастний випадок. У нормальному стані USB 2.0-клавіатура має слабкий електромагнітний витік, а після ремонту електромагнітний витік добре видно.

Які саме клавіші ви досліджували?

Ми зібрали великий набір даних для 70 часто вживаних клавіш: цифри 0–9, усі літери a–z і A–Z, а також крапка, кома, пробіл, backspace, CTRL, ALT, SHIFT і ENTER. Це важливо, бо робота показує не демонстрацію на двох-трьох символах, а повноцінний словник натискань, достатній для реального текстового введення.

У яких умовах ви перевіряли атаку?

У трьох різних середовищах. Перше – відкритий простір, фактично де майже немає елементів, які могли б сприяти додатковому електромагнітному зв'язку. Друге – за межами офісної кімнати, коли ціль розташована всередині, а приймач – у коридорі. Третє – зовні будівлі, тобто ще більш реалістичний сценарій зовнішнього спостереження. Саме ця різноманітність середовищ робить результати особливо цінними.

Наскільки далеко вдавалося виявляти натискання?

Найсильніший результат був отриманий у сценарії поза офісною кімнатою: там вдалося досягти приблизно 100% точності на відстані в 12 м, причому між передавачем і приймачем була ще й стіна товщиною14 см. У відкритому просторі надійний діапазон був близько 3.8 м, а зовні будівлі – близько 9.4 м.

Чому в коридорі результат кращий, ніж у відкритому просторі?

Тому що середовище саме починає допомагати хвилі. У статті прямо зазначено, що в офісному середовищі є багато електронних пристроїв та елементів, з якими випромінювання може зчіплюватися, а коридор частково поводиться як хвилевод, полегшуючи поширення хвилі. Тобто парадоксально, але складніше середовище іноді не гасить витік, а робить його ще практичним для далекого спостереження.

Яким був сам експериментальний тракт?

Для знімання бездротового випромінювання використовувалася антена, низько шумний підсилювач та осцилограф. Одночасно два дротові канали осцилографа підключалися до DATA+ і DATA−, щоб отримати опорний дротовий сигнал і синхронізувати події всередині кадру. Далі бездротовий сигнал оброблявся окремо.

А як ви перетворювали прийнятий сигнал на конкретну клавішу?

Ми не намагалися “розпізнавати звук” або будувати громіздку нейромережу. Натомість розробили доволі ефективний алгоритм на основі послідовності фронтів. Спочатку з дротового сигналу DATA+ формувалася еталонна бітова послідовність фронтів для кожної з 70 клавіш. Для цього сигнал фільтрували, диференціювали, виділяли піки й перетворювали на бінарну послідовність, де “1” означає наявність фронту, а “0” – його відсутність. Потім бездротовий сигнал проходив через смуговий фільтр, нормалізацію, придушення шуму, детектор піків – і з нього теж будувалася послідовність фронтів. Далі система просто шукала, яка з 70 еталонних послідовностей збігається найкраще.

Чому ви називаєте цей алгоритм ефективнішим?

Тому що він не потребує важкої спектрограмної обробки чи складної моделі машинного навчання для кожного спостереження. Значна частина роботи – побудова еталонної серії фронтів – виконується один раз. Після цього в реальному часі потрібно лише профільтрувати бездротовий сигнал, знайти піки, сформувати серію фронтів і порівняти її з готовими шаблонами. Для сценарію, де клавіатура опитується з інтервалом близько 1 мс, така економність алгоритму є дуже важливою.

Які фактори найбільше впливають на результат?

У статті детально аналізуються два: велике зовнішнє завадове збурення і ємнісний зв’язок через тіло людини. Завада може породжувати великі паразитні піки, які інколи збивають піковий детектор і призводять до хибних “1” у серії фронтів. Ємнісний зв’язок через тіло людини, навпаки, іноді покращує прийом: якщо людина торкається непровідної частини приймальної антени, амплітуда сигналу може зрости в 2–4 рази. Це означає, що людське тіло може випадково або навмисно стати частиною приймальної системи.

Які контрзаходи ви розглядали?

Ми протестували зовнішнє екранування відремонтованої ділянки за допомогою восьми шарів

алюмінієвої фольги. Це зменшило потужність випромінювання на 30 дБ, але не прибрало його повністю. Тобто зовнішнє багатошарове металеве екранування під час ремонту справді допомагає, але не є абсолютним рішенням.

То який практичний урок із цього для реальних об'єктів?

Дуже простий і дуже неприємний: навіть звичайна польова або "тимчасова" апаратна модифікація може створити нову поверхню атаки. У статті прямо згадуються реальні ситуації, де через логістичні або регуляторні обмеження персонал часто змушений ремонтувати кабелі замість їх заміни. Саме в таких умовах ризик особливо високий: ремонт повертає працездатність, але непомітно погіршує електромагнітну безпеку.

Який головний висновок вашої роботи?

Що ремонт кабелю – це не тільки електричне, а й електромагнітне втручання. Ми показали, що апаратна модифікація, яка для користувача виглядає невинною, може різко посилити побічні електромагнітні випромінювання і дати можливість дистанційного відновлення натискань клавіш. Тобто нова вразливість виникає не через програмну помилку і не через закладку, а через зміну конструкції звичайного кабелю.

Чому це важливо вже зараз

Ця робота особливо цінна тим, що вона переносить увагу з "пристрою як такого" на його життєвий цикл. Ми часто оцінюємо безпеку клавіатури, комп'ютера чи кабелю в заводському стані. Але реальна експлуатація майже ніколи не буває ідеальною: кабелі ламаються, ремонтуються, перетискаються, втрачають екранування, змінюють форму. І саме в цих дрібних нештатних змінах може народитися канал витоку, який не передбачали ні виробник, ні користувач.

Фінальний висновок

Стаття Keystroke Detection by Exploiting Unintended RF Emission from Repaired USB Keyboards показує що в сучасній технічній безпеці: інколи нова вразливість виникає не тоді, коли систему зламали, а тоді, коли її просто полагодили. У світі TEMPEST це особливо небезпечно, бо межа між “ремонтом” і “формуванням випромінювача” може бути тоншою, ніж здається. І якщо звичайне скручування або пайка здатні перетворити кабель на антену, то справжній захист починається вже не лише з вибору пристрою, а з культури його обслуговування, ремонту й післяремонтного контролю.

Як нова теорема про побічні канали витоку в зашифрованому трафіку змінює саму логіку захисту [10]

Є бажання вірити, що сучасне шифрування нарешті зробило мережевий трафік "захищеним". TLS 1.3 приховує вміст, QUIC закриває ще більше деталей, а сильні криптографічні примітиви начебто не залишають місця для змістовного спостереження. Але саме тут починається найцікавіше. Стаття The Inevitability of Side-Channel Leakage in Encrypted Traffic ставить не прикладне, а майже філософське запитання: якщо корисний вміст уже зашифрований, то чому аналіз трафіка усе ще працює? І відповідає на нього не евристично, а строго – через формальну модель, нерівність обробки даних, взаємну інформацію і доведення теореми існування побічних каналів витоку. Головний висновок звучить жорстко: в ефективних, придатних до реального використання системах побічний витік у зашифрованому трафіку не є випадковим дефектом. Він є неминучим.

У чому головна ідея вашої роботи?

Ми хотіли дати суворе теоретичне обґрунтування тому, що давно спостерігається на практиці: навіть коли корисне навантаження трафіку надійно зашифроване, побічні ознаки трафіку все одно несуть інформацію про його зміст або семантику. Головний внесок нашої роботи в тому, що ми не просто констатуємо цей факт, а будуємо формальну модель зашифрованої комунікаційної системи й доводимо теорему існування побічних каналів, яка показує: за певних, дуже природних для реальних мереж умов, взаємна інформація між спостережуваними ознаками трафіку і прихованою семантикою обов'язково є строго додатною.

Тобто ви намагаєтеся відповісти не на питання "як атакують", а на питання "чому це взагалі можливо"?

Саме так. Дуже багато робіт з аналізу трафіка показують високі точності класифікації – для цифрових відбитків веб-сайтів, для ідентифікації програмного забезпечення, для деанонімізації. Але при цьому довгий час бракувало строгої відповіді на фундаментальне питання: чому витоки побічними каналами взагалі не зникають після шифрування?

Наша стаття саме про це. Вона не просто описує окрему атаку, а закладає інформаційно-теоретичний фундамент існування такого витоку.

Чому проблема стала особливо актуальною зараз?

Тому що сучасні протоколи, як-от TLS 1.3 і QUIC, фактично закрили прямий доступ до вмісту повідомлень. Це змістило центр ваги від аналізу змісту до аналізу побічних ознак: довжин пакетів, їхнього напрямку, часових інтервалів, burst-структури, частоти обміну, поведінки протоколу. І саме тому сьогодні потрібно не просто емпірично показувати, що витік існує, а строго розуміти межі цього витоку. У вступі ми прямо зазначаємо, що вміст став невидимим, але аналіз трафіка продовжує показувати дуже високі результати.

Яким є ваш основний інтуїтивний аргумент?

Інтуїція дуже проста: шифрування змінює вміст, але не може безкінечно змінювати метадані процесу передачі, якщо система хоче залишатися ефективною, сумісною та корисною. Протокол усе ще повинен маршрутизувати пакети, підтримувати контроль потоку, дотримуватися обмежень MTU, працювати в прийнятних затримках, зберігати пропускну здатність. А отже, довжини, часи, напрямки й статистичні патерни трафіку не можуть бути довільно зруйновані. Саме в цій неминучій структурі й народжується побічний канал.

А що таке невиродженість відображення? Це звучить доволі технічно.

Це один із центральних елементів статті. Він означає, що відображення від протокольного рівня до реально спостережуваного мережевого трафіку не може надто сильно "спотворити" статистичну структуру. Формально ми вводимо константу C, яка обмежує очікуване відхилення між протокольними траєкторіями та мережевими траєкторіями в деякій метриці. Глибша ідея така: якщо система хоче зберігати ефективність, то вона не може довільно ламати власний трафік – інакше зруйнуються

затримки, пропускна здатність, швидкість або сумісність із реальною мережею. Саме тому C у реальних системах не може стати нескінченним: ефективність стримує ступінь обфускації.

Тобто ефективність тут стає ворогом повної приватності?

Саме це ми й показуємо. І це один із головних висновків роботи. У реальних системах витік побічними каналами неможливо прибрати повністю, бо будь-яка сильна спроба обнулити розрізнюваність або різко збільшити спотворення відображення відразу б'є по пропускній здатності каналу, швидкості передачі і функціональності. У цьому сенсі витік побічними каналами – це не просто слабке місце реалізації, а наслідок проєктування системи з пріоритетом ефективності.

Як перейти від "позитивної взаємної інформації" до реальної успішної атаки?

Це дуже важливий момент. У розділі 5 ми показуємо, як перейти до нижньої межі повної точності ідентифікації в бінарному випадку, а також як працює ефект накопичення спостережень. Якщо є кілька незалежних сесій або кілька часових вікон, взаємна інформація накопичується, і точність ідентифікації зростає. У статті це пов'язано і з нерівністю Фано, і з інформацією Чернова. Тобто наш результат не обмежується абстрактною тезою "витік існує", а дає операційну інтерпретацію: якщо в системі є хоч трохи стійкого витоку, то за достатнього бюджету спостережень атака неминуче стає сильнішою.

Чи означає це, що довгі спостереження майже завжди грають на боці атакувальника?

Так. Саме це ми і підкреслюємо. Якщо дані з різних сесій або вікон можна накопичувати, то витік не просто існує, а акумулюється. У розділі 5 прямо сказано, що при незалежних спостереженнях взаємна інформація додається, а ймовірність похибки спадає експоненційно. Це дає дуже важливий практичний висновок: навіть невеликий витік, якщо він стабільний, з часом може стати дуже небезпечним.

Який найсильніший концептуальний результат статті?

Напевно, те, що ми зміщуємо мову обговорення. Більшість дискусій про аналіз трафіка точаться навколо конкретних атак і конкретних схем захисту. Ми ж показуємо, що правильне питання звучить не "чи існує витік", а "яку саме нижню межу витоку диктує система своєю межею ефективності". Інакше кажучи, нульовий витік у практичній системі – це не реалістична мета. Реалістична мета – це оптимізація з обмеженнями: мінімізувати витік, не руйнуючи корисність системи. У фіналі статті це прямо оформлено як правильну інженерну ціль.

Що ваша теорія говорить про захисти на кшталт вирівнювання пакетів, маскування трафіку або диференційної приватності?

Вона не заперечує їхню цінність, але ставить їх у правильний контекст. Усі ці механізми можуть зменшувати витік, але не відміняють фундаментальну межу. Вирівнювання пакетів збільшує C, але ціною пропускної здатності. Навмисне спотворення часових інтервалів збільшує затримки. Маскування трафіку допомагає, але дорого обходиться по обсягу передавання. А диференційна приватність сама по собі теж не усуває теоретичну проблему – вона лише формалізує компроміс. Ми прямо пишемо, що правильна інженерна задача – це мінімізувати витік за заданих обмежень на пропускну здатність, збільшення затримки і збереження функціональності.

Отже, "повна приватність" для зашифрованого трафіку – це ілюзія?

Для ефективних, реальних, сумісних із мережею систем – так, саме так. Принаймні в тому строгому сенсі, який ми розглядаємо. Якщо система повинна бути корисною, швидкою, сумісною й підтримувати різноманітні застосунки, вона не може довільно зруйнувати всю статистичну структуру свого трафіку. А значить, якийсь побічний слід обов'язково залишиться. Це і є зміст слова inevitability в назві нашої роботи.

Який головний висновок ви хочете залишити читачеві?

Що побічні витоки в зашифрованому трафіку – це не ексцес, не випадкова помилка й не просто тимчасова недопрацьованість окремого протоколу. Це структурний наслідок того, що реальні системи одночасно повинні бути і безпечними, і корисними, і ефективними. І якщо ми це визнаємо, тоді змінюється сама постановка задачі: не "знищити витоки повністю", а "знати його нижню межу, уміти її оцінювати й проектувати систему усвідомлено".

Чому це важливо вже сьогодні

Ця стаття важлива не лише для дослідників з аналізу трафіку. Вона важлива для всіх, хто проектує мережеві системи, анонімні канали, VPN, захисні проксі й обфускаційні механізми. Бо вона змінює саме мислення про проблему. Після цієї роботи вже складніше вдавати, що витік побічними каналами – це просто "те, що ще не встигли полагодити". Натомість перед нами постає тверезіша картина: витік є фундаментальним побічним продуктом корисної комунікації, а значить інженер повинен працювати не з ілюзією абсолютного приховування, а з математично неминучим компромісом.

Фінальний висновок

Стаття The Inevitability of Side-Channel Leakage in Encrypted Traffic робить рідкісну річ: вона не просто додає ще одну атаку до довгого списку робіт з аналізу трафіку, а пояснює, чому весь цей список взагалі не міг не з'явитися. Вона показує, що в сучасних мережах шифрування приховує зміст повідомлення, але не може нескінченно приховувати сам факт, ритм, структуру й форму спілкування – якщо система хоче залишатися швидкою, функціональною та придатною до використання. І саме тому справжня зрілість у захисті починається не з мрії про нульовий витік, а з готовності визнати його неминучість, виміряти його межі й будувати оборону всередині цього жорсткого, але чесного математичного світу.

Як побічні електромагнітні випромінювання комп'ютера дозволяють відновлювати зображення без доступу до самого дисплея [11]

Ідея, що комп'ютер може передавати назовні дані навіть тоді, коли ніхто не підключається до його мережі, звучить як сюжет із технічного трилера. Але для TEMPEST це майже класика. Щойно електроніка починає працювати з відеосигналом, вона мимоволі створює побічне електромагнітне випромінювання. І якщо це випромінювання правильно перехопити, синхронізувати й обробити, є можливість відновити те, що, здавалося б, залишилося лише на екрані. Стаття Reconstruction of Video Electromagnetic Leakage from Computer цікава тим, що показує не просто факт існування такого витоку, а повноцінну інженерну схему його відновлення: від приймання побічного сигналу до реконструкції текстового зображення. Для сучасного читача це важливе нагадування: у сфері інформаційної безпеки проблема не закінчується там, де починається шифрування чи фізична ізоляція. Інколи сам дисплей уже є джерелом витоку.

У чому головна ідея вашої роботи?

Головна ідея полягає в тому, що побічне електромагнітне випромінювання комп'ютера, зокрема відеотракту, може містити достатньо інформації для відновлення зображення, яке виводиться на екран. У статті ми не обмежуємося загальною тезою про небезпеку TEMPEST, а проєктуємо систему перехоплення й реконструкції відеоелектромагнітного витоку, яка дозволяє після приймання сигналу виконати синхронізацію, фільтрацію, фазове підстроювання й у підсумку відновити текстове зображення.

Чому саме відеоканал комп'ютера є таким важливим джерелом витоку?

Тому що саме відеодисплейний тракт є прямим інтерфейсом взаємодії людини з машиною. Через нього проходить інформація, яку користувач безпосередньо сприймає як зображення на екрані. У статті прямо сказано, що відеоканал є однією з найважливіших частин комп'ютера з погляду можливого витоку, оскільки його електромагнітне

випромінювання містить відображувану інформацію. Це робить відеоканал одним із найнебезпечніших каналів TEMPEST-витоку.

Чому взагалі електроніка починає "випромінювати" інформацію?

Тому що вся електронна обробка даних зводиться до керування змінами струму або напруги. А змінний струм неминуче породжує електромагнітне випромінювання. У статті підкреслюється, що ці випромінювання містять багатий спектральний склад і можуть нести інформацію, яку потенційно можна виділити й дешифрувати. Іншими словами, витік виникає не як аномалія, а як фізичний супровід нормальної роботи цифрової системи.

У вашій статті відчувається, що TEMPEST розглядається не просто як технічна деталь, а як окремий клас загроз. Чому?

Тому що TEMPEST не зводиться до самого факту випромінювання. Його суть у тому, що з цих побічних електромагнітних проявів можна виділити корисну інформацію. У вступі прямо сказано, що TEMPEST – це не просто проблема електромагнітних завад, а технологія, пов'язана з перехопленням комп'ютерної інформації через побічні випромінювання, яка становить серйозну загрозу для інформаційної безпеки й електронного протиборства.

Які саме джерела витоку всередині комп'ютера ви вважаєте основними?

У роботі зазначено, що джерелами електромагнітного випромінювання можуть бути CPU, комунікаційні кола, перетворювальні вузли, вихідні пристрої та інші елементи системи. Вони можуть породжувати різні типи сигналів витоку: синхросигнали, тактові сигнали, цифрові сигнали обробки та безпосередньо інформацію, що відображається на екрані. Але саме відеосигнал є особливо небезпечним, бо він несе інформацію в структурі, яка порівняно легко пов'язується з видимим зображенням.

Що саме ви побудували у своїй роботі?

Ми спроєктували систему перехоплення і відновлення для відеоелектромагнітного витоку комп'ютера. Після перехоплення побічного сигналу система переводить його в цифрову форму і далі обробляє програмно. У тексті сказано, що після широкосмугового приймання сигнал дискретизується із частотою 60 МГц, а потім обробляється для виділення кадрової синхронізації, рядкової синхронізації й самого відеосигналу. Це дозволяє відновити текстове зображення з електромагнітного витоку.

Чому синхронізація є такою важливою?

Тому що без правильного виділення кадрових і рядкових синхросигналів неможливо відновити геометрію зображення. У статті окремо зазначено, що одним із ключових етапів реконструкції є виділення синхроімпульсів із сигналу витоку. Саме вони дозволяють правильно розмістити відновлений відеосигнал у структурі кадру й побачити на екрані не хаотичний шум, а осмислене текстове або графічне представлення.

Які методи обробки сигналу ви вважаєте основними?

У статті прямо названо кілька ключових методів: синхронізація, кореляційна фільтрація, фазове автопідстроювання, а також методи узгодженої фільтрації для підвищення відношення сигнал/шум. На четвертій сторінці окремо пояснюється цифрове фазове автопідстроювання як метод стабілізації синхросигналів, а також метод кореляційної фільтрації, який дозволяє підвищити відношення сигнал/шум за рахунок накопичення періодичної структури сигналу. Саме поєднання цих методів робить слабкий і спотворений побічний сигнал придатним для реконструкції.

Чому взагалі обробка такого сигналу є складнішою, ніж у звичайному радіозв'язку?

Тому що сигнал побічного витоку – це не класичний канал зв'язку, який спочатку проєктувався для стійкого передавання інформації. У статті прямо зазначено, що прийнятий сигнал витоку має низьке відношення сигнал/шум, широкий спектр і додатково спотворюється під час проходження бездротовим каналом. Через це його приймання й обробка теоретично й технічно відрізняються від звичайного радіоприймання. Тут не можна просто "налаштуватися на частоту"; потрібен набір відновлювальних процедур, які буквально збирають сигнал заново.

Який практичний результат вам вдалося отримати?

У роботі прямо сказано, що за допомогою описаної системи вдалося відновити текстове зображення з електромагнітного витоку на відстані 10 метрів. Автор подає це як важливий результат і навіть називає його проривом порівняно з ранішими обмеженішими дистанціями. Для TEMPEST-сценарію це принципово: йдеться вже не про лабораторний контактний вимір, а про дистанційне відновлення видимого змісту екрана.

У статті є історичний контекст. Чому ви його включили?

Бо тема TEMPEST має довгу історію, і важливо показати, що проблема не є новою чи випадковою. У вступі згадуються ранні демонстрації відновлення екранного вмісту за допомогою телевізійних приймачів, праці Van Eck і результати інших дослідницьких груп. Це потрібно не лише для історичної довідки, а й для того, щоб підкреслити: сучасна робота стоїть у довгій лінії досліджень, які послідовно доводили, що побічні випромінювання відеотракту можуть бути використані для практичного шпигунства.

Що у вашій роботі є головним джерелом загрози для інформаційної безпеки?

Не просто саме випромінювання, а його інформативність. Якщо б побічний сигнал не зберігав структури відображуваного зображення, він був би лише електромагнітним фоном. Але в нашому

випадку він зберігає синхронізацію, елементи відеоструктури й дозволяє відновлювати текстову інформацію. Тому загроза полягає не в наявності електромагнітного поля як такого, а в тому, що воно є корельованим із корисною інформацією. Саме цю думку стаття послідовно проводить від вступу до технічної частини.

Який головний висновок ви б хотіли залишити читачеві?

Що комп'ютерний дисплей не можна розглядати лише як засіб виведення інформації. З точки зору TEMPEST він одночасно є і джерелом побічного електромагнітного витоку. Наша робота показує, що за певних умов цей витік можна не просто виявити, а використати для реконструкції текстового зображення. Це означає, що захист інформації має враховувати не лише програмний або мережевий рівень, а й фізичну сторону роботи системи.

Чому це важливо вже сьогодні

Попри те що стаття була опублікована ще у 2007 році, її інтелектуальне ядро зовсім не застаріло. Навпаки, сьогодні воно читається ще гостріше. Ми живемо в епоху, коли дедалі більше уваги приділяється побічним каналам, SDR, машинному навчанню для реконструкції сигналів і високочутливим засобам приймання. У такому контексті ранні роботи з відновлення відеоелектромагнітного витоку набувають нового змісту: вони показують базову фізику проблеми, яку сучасні алгоритми можуть зробити ще небезпечнішою.

Фінальний висновок

Стаття Reconstruction of Video Electromagnetic Leakage from Computer нагадує про одну з найнеприємніших істин технічного захисту: інформація витікає не лише через канали, які ми проклали навмисно, а й через ті, що створює сама фізика роботи електроніки. Екран комп'ютера може бути не тільки вікном, через яке людина бачить дані, а й джерелом побічного випромінювання, через яке ці дані бачить хтось інший. І саме тому справжній захист починається там, де ми перестаємо сприймати апаратуру як "нейтральну" і починаємо бачити в ній активного учасника інформаційного витоку.

Як правильний вибір рівня сигналу дозволяє залишити зв'язок усередині контрольованої зони й одночасно позбавити противника можливості перехоплення [12]

У технічному захисті інформації є бажання мислити великими категоріями: екранування, завади, криптографія, складні системи контролю. Але інколи вирішальне питання звучить значно простіше: яким саме має бути рівень сигналу, щоб свій приймач ще впевнено його бачив, а засоби технічної розвідки за межами контрольованої зони – вже ні. Саме цю логіку розгортає стаття Determination of Signal Level for Protection of Information in Case of Its Interception by Technical Means of Intelligence. Її сила не в екзотичних методах, а в дуже практичній інженерній постановці: якщо відомі відстань до легітимного приймача та характеристики його антени, то можна розрахувати такий рівень випромінювання, який буде достатнім для нормальної роботи всередині захищеної зони, але недостатнім для перехоплення зовні. Це вже не пасивний захист, а точне дозування самої можливості витоку.

У чому головна ідея вашої роботи?

Головна ідея полягає у визначенні такого рівня вихідного сигналу, який забезпечує надійне приймання всередині контрольованої зони, але не дозволяє технічним засобам розвідки перехопити його за її межами. У статті це прямо сформульовано як спосіб захисту інформації в умовах її перехоплення технічними засобами розвідки: не просто аналізувати канал витоку, а математично визначити допустимий рівень випромінювання.

Чому саме рівень сигналу стає засобом захисту?

Тому що будь-яке перехоплення починається не з "розуміння" змісту сигналу, а з самого факту його виявлення на вході приймача розвідки. Якщо сигнал за межами контрольованої зони не досягає порогового рівня виявлення, то далі вже немає що аналізувати. У статті саме це і закладено: потрібно забезпечити таку енергетику каналу, щоб свій приймач працював, а сторонній – ні. Це дуже прагматичний підхід до технічного захисту.

На яку модель ви спираєтесь у дослідженні?

У роботі використано існуючу математичну модель перехоплення сигналу засобами радіотехнічної розвідки. Вона включає три головні блоки: розрахунок відношення сигнал/шум на вході приймача перехоплення, опис перетворення сигналу елементами радіоприймача та блок оцінювання інформаційного показника, що характеризує ефективність приймача розвідки. На цій основі вже будується захисна інтерпретація моделі.

У статті багато уваги приділено схемі виявлення сигналу на фоні шуму. Чому це так важливо?

Тому що саме на рівні детектора приймається базове рішення: сигнал є чи сигналу немає. Автор розглядає оптимальну схему виявлення детермінованого сигналу на фоні білого шуму й показує чотири можливі сценарії: два правильні рішення і два помилкові. Для захисту найбільш цікавий саме останній випадок – коли сигнал присутній, але поріг не досягається, і технічний засіб розвідки робить висновок, що сигналу немає.

Тобто захисна логіка базується на тому, щоб перевести противника в режим пропуску сигналу?

Саме так. У статті це фактично і є ключовою інженерною ідеєю. Якщо забезпечити такий рівень випромінювання, за якого за межами контрольованої зони сигнал не перевищує поріг приймача технічної розвідки, то реалізується сценарій: сигнал формально існує, але для засобу розвідки він “невидимий”. Це і є одна з можливих форм активного обмеження витоку.

Який саме ключовий результат ви отримали?

Головний результат – це залежність для розрахунку такого рівня вихідного сигналу, який є достатнім для роботи штатного приймача, але недостатнім для технічних засобів розвідки поза межами контрольованої зони. У статті ця залежність виражена через відстань між передавачем і приймачем,

довжину хвилі, коефіцієнт підсилення приймальної антени та інші параметри. Саме на її основі будується методика захисту.

Тобто метод дозволяє не просто сказати "зменшіть потужність", а оцінити її обґрунтовано?

Саме в цьому і сенс. Просте зменшення потужності "на око" може або не захистити від перехоплення, або зірвати роботу власного каналу. У статті ж пропонується не інтуїція, а розрахунковий підхід: якщо відомі відстань до свого приймача та максимальний коефіцієнт підсилення його антени, можна оцінити параметри передавання так, щоб сигнал залишався працездатним у межах контрольованої зони й одночасно не перетинав поріг розвідки за її межами.

У чому практичний сенс такого підходу для систем технічного захисту інформації?

У тому, що він дозволяє працювати не лише з наслідками витоку, а з його енергетичною причиною. Багато засобів захисту діють уже після того, як сигнал став доступним для спостереження: шифрування, маскування, завади. Тут підхід інший: зробити так, щоб небезпечний приймач узагалі не отримав сигнал із достатнім рівнем. Це дуже важливо для задач, де канал зв'язку сам по собі повинен існувати, але не повинен "вилазити" за межі контрольованого простору.

Які обмеження ви самі бачите в цьому методі?

У статті це сказано прямо: обмеженням є необхідність постійного врахування й перерахунку відстані між передавачем і приймачем, а також відповідного максимального коефіцієнта підсилення приймальної антени. Іншими словами, метод добре працює там, де геометрія системи та її параметри достатньо відомі й контрольовані. Якщо ж просторові умови або характеристики приймання змінюються непередбачувано, потрібна або адаптація, або автоматизація такого розрахунку.

Ви вказуєте напрям подальших досліджень. У чому він полягає?

Подальший крок – це автоматичне визначення бажаного рівня сигналу для захисту від перехоплення технічними засобами розвідки. У статті прямо сказано, що майбутні дослідження мають бути спрямовані на розробку засобів автоматичного визначення потрібного рівня сигналу. Тобто йдеться про перехід від статичної формули до адаптивної системи, яка могла б у реальному часі підтримувати безпечний рівень випромінювання.

Який головний висновок вашої статті?

Що одним із реальних способів захисту інформації від перехоплення технічними засобами розвідки є правильне визначення рівня сигналу передавання. Якщо сигнал достатній для свого приймача, але не досягає порогу виявлення зовнішнього приймача за межами контрольованої зони, то це вже дає практичний захисний ефект. У висновках статті прямо сказано, що за такої умови засоби технічної розвідки поза межами контрольованої зони не зможуть досягти порогового рівня, а отже буде забезпечено захист вихідного сигналу.

Чому це важливо вже сьогодні

Сила цієї роботи в тому, що вона повертає технічний захист інформації до дуже фундаментального питання: не будь-який сигнал, який ми передаємо, повинен бути “максимально сильним”. У сфері безпеки надлишкова енергія випромінювання може означати не кращий зв’язок, а більший радіус витоку. І саме тому задача захисту тут перетворюється на задачу точного налаштування: дати рівно стільки енергії, скільки потрібно своїй системі, але не більше, ніж потрібно потенційному противнику.

Фінальний висновок

Стаття Determination of Signal Level for Protection of Information in Case of Its Interception by Technical Means of Intelligence показує важливу й дуже інженерну істину: інколи захист починається не з ускладнення системи, а з її точнішого

налаштування. Якщо ми вміємо розраховувати межу, за якою корисний сигнал неможливо перехопити, то отримуємо не абстрактну “безпеку”, а конкретний керований параметр захисту. І в цьому сенсі правильний рівень сигналу – це вже не лише характеристика передавача, а частина архітектури інформаційної оборони.

Як VGA\HDMI – кабель перетворюється на передавач, а звичайні LoRa-шлюзи – на приймачі прихованого витоку [13]

Велика мінімальна відстань між пристроєм обробки інформації та місцями можливого розташування засобів технічної розвідки довгий час вважається панацеєю щодо захисту інформації від її витоку: якщо комп'ютер фізично ізольований від мережі, то винести з нього дані назовні стає вкрай важко. Але стаття TEMPEST-LoRa: Cross-Technology Covert Communication показує тривожну зміну правил гри. Автори демонструють не просто ще один TEMPEST-канал, а новий тип міжтехнологічного прихованого зв'язку, в якому побічне електромагнітне випромінювання відеокабелю навмисно перетворюється на LoRa-сумісні пакети, здатні прийматися звичайними комерційними LoRa-вузлами та шлюзами. Інакше кажучи, кабель VGA або HDMI тут уже не просто "випромінює" – він починає імітувати бездротовий протокол далекого радіуса дії. Саме це і робить роботу особливо небезпечною: нападнику більше не обов'язково ставити поруч дорогий спеціалізований SDR-приймач – він може використовувати вже наявну LoRa-інфраструктуру.

У чому головна ідея вашої роботи?

Ми показали новий електромагнітний канал, який дозволяє передавати дані з захищеного комп'ютера до звичайних LoRa-приймачів. Головна ідея полягає в тому, щоб керовано модулювати побічне випромінювання відеокабелю – VGA або HDMI – так, щоб воно стало сумісним із фізичним рівнем LoRa. У результаті електромагнітний-витік перестає бути просто побічним явищем і стає носієм повноцінних LoRa-подібних пакетів.

Чому це небезпечніше за попередні TEMPEST-атаки?

Тому що більшість попередніх електромагнітних каналів вимагали дуже близького розташування приймача та використання спеціалізованого обладнання. У нашому випадку приймачем можуть бути пристрої для бездротового зв'язку за технологією LoRa уже розгорнуті в реальному середовищі. Це різко знижує вартість атаки і розширює її практичний радіус дії. Саме цей перехід від "спеціального шпигунського приймача" до "звичайної LoRa-інфраструктури" і є головною проблемою.

Тобто ви фактично поєднали TEMPEST і бездротовий обмін даними?

Саме так. У цьому і полягає новизна роботи. Ми не просто використовуємо побічне електромагнітне випромінювання, як канал, а інтегруємо його з логікою бездротового обміну даними. Це дозволяє передавати дані від відеокабелю до LoRa-пристрою, тобто між двома фізично різними технологічними середовищами. Автори прямо зазначають, що TEMPEST-LoRa є першим прикладом такої інтеграції для комерційного бездротового протоколу.

Чому джерелом витоку ви обрали саме відеокабель?

Тому що відеокабель уже давно відомий як сильне джерело контрольованого електромагнітного-випромінювання. Тому ми повернулися до моделі електромагнітного випромінювання відеокабелів і розробили дуже точне керування випромінюванням на рівні піксельного потоку. Це дозволило використовувати відеокабель як своєрідна передавальна антена.

Що означає "відеокабель як передавальна антен"?

Це одна з найсильніших інженерних ідей статті. Передавання зображення через відеокабель уже означає, що графічна карта формує цифровий потік пікселів, а на кабелі виникають відповідні зміни напруги. Ми показуємо, що цей процес можна інтерпретувати як аналог цифрового дискретного радіопередавача: піксельний потік стає базовим цифровим сигналом, напруга на шині – аналоговим представленням, а сам кабель виконує роль антени.

Але частота випромінювання кабелю значно нижча за робочу частоту LoRa, наприклад 915 МГц. Як ви обходите цю проблему?

Через гармоніки випромінювання. Це ключовий технічний момент. Сама частота випромінювання кабелю для типового режиму 1080×1920@60Hz становить 148.5 МГц, але випромінювання кабелю містить не лише основну частоту, а й її гармоніки. Ми

використовуємо спеціально сформовані зображення, щоб керувати характеристиками електромагнітного випромінювання на гармоніках і таким чином зміщувати енергію в цільові LoRa-діапазони, зокрема 433–470 МГц та 868–915 МГц.

Як саме формується таке випромінювання?

Через спеціально створене зображення. Автори пропонують алгоритм, який формує піксельний потік так, щоб через чергування чорних і білих пікселів створювати потрібні частотні характеристики електромагнітного випромінювання. Алгоритм генерує зображення для цільових частот, а далі ці частоти використовуються як будівельні блоки для LoRa-подібних сигналів. Чорно-білий патерн тут важливий тому, що дає максимальну інтенсивність випромінювання.

Тобто ви фактично керуєте випромінюванням на рівні піксельної структури кадру?

Так. Саме в цьому і полягає точне керування. Ми працюємо не з грубою зміною цілого зображення, а з точним формуванням піксельного потоку, який змінює частотні характеристики електромагнітного випромінювання настільки точно, що з нього можна побудувати LoRa-радіосигнали. Це вже не просто "витік від картинки", а програмоване формування протокольно сумісного бездротового сигналу.

Як ви робите електромагнітне випромінювання сумісним саме з LoRa?

Для цього ми модулюємо електромагнітне випромінювання випромінювання так, щоб воно повторювало логіку протоколу роботи пристрою LoRa (CSS). Ми формуємо електромагнітний сигнал, який відповідає BW (смузі пропускання) і SF (швидкості передачі) LoRa-приймача.

Наскільки універсальним є цей підхід для LoRa-параметрів?

Автори прямо наголошують, що TEMPEST-LoRa здатна генерувати сигнали, сумісні з усіма комбінаціями BW і SF, які використовуються комерційними LoRa-пристроями. Це дуже важливо, бо означає, що нападник не прив'язаний до одного вузького профілю приймача, а потенційно може підлаштовуватися під широку множину вже розгорнутих LoRa-пристроїв.

Який реальний радіус і швидкість передачі ви отримали?

Згідно з основними результатами, сигнал від LoRa-пристрою можна було надійно декодувати на відстані до 87.5 м або передавати зі швидкістю до 21.6 біт за секунду.

Ви згадуєте, що сигнал може проходити крізь бетонні стіни. Це справді показано в роботі?

Так. Автори прямо пишуть, що LoRa-подібні EM сигнали можуть «проходити» стіни і зберігати достатню силу завдяки високій завадостійкості LoRa-сигналів та високій чутливості LoRa-примачів. Саме це й робить атаку особливо реальною для фізично ізольованих приміщень: сигнал не обов'язково мусить виходити у "чистий ефір", щоб бути корисним.

У цій статті є ще одна майже шпигунська деталь – монітор може бути вимкнений, а передавання триватиме?

Саме так. Це один із найтривожніших моментів. Автори показують, що через спеціальні програми для керування монітором можна змінити параметри монітор (яскравість, контрастність, колірну температуру) монітора так, щоб екран став чорним, але відеокабель продовжував передавати піксельний потік і випромінювати електромагнітний сигнал. Отже, передача може виконуватися з вимкненим на вигляд дисплеєм, що різко підвищує прихованість атаки.

Яку модель загроз ви вважаєте реалістичною?

Модель загроз досить жорстка, але цілком реалістична. Припускається, що на ізольований комп'ютер уже впроваджено шпигунське програмне забезпечення. Далі шкідливий код знаходить конфіденційні файли, шифрує їх для нападника і, коли комп'ютер залишається без нагляду, запускає перетворення сигналу. Поруч при цьому можуть бути звичайні LoRa-пристрої, які в реальних об'єктах часто не вважаються критичними з точки зору захищеності.

Чому присутність LoRa-пристроїв поблизу ви вважаєте реалістичною?

Тому що в сучасних будівлях та інфраструктурі LoRa-пристрої широко використовується для різних задач: пожежна, охоронна сигналізація, промислові датчики під спеціальні цілі та інше. Автори наголошують, що стандарти захисту інформації від її витоку зазвичай вимагають від'єднання Wi-Fi, Bluetooth, Ethernet та інших прямих комунікаційних інтерфейсів самого комп'ютера, але не завжди вимагають очищення навколишнього простору від комерційних бездротових пристроїв на десятки метрів навколо. Саме тут і виникає нова зона ризику.

Які практичні труднощі вам довелося долати?

Одна з важливих проблем – інтервал кадрів. Коли один електромагнітний сигнал не вміщується в межі одного відеокадру, TEMPEST-LoRa має об'єднувати кілька кадрів у відео. Але між кадрами є неминучий проміжок приблизно 0.673 мс, який може ламати безперервність сигналу і спричиняти помилки декодування.

Але попри це пакети все одно декодуються?

Так, і саме це показує практичну життєздатність атаки. Автори пояснюють, що фізичний рівень LoRa використовує механізми корекції помилок, тому навіть електромагнітні сигнали з інтервалом кадрів у багатьох випадках можуть бути успішно декодовані. Тобто природні характеристики відеокадру шкодять каналу, але не знищують його.

Чому ваша атака така сильна саме концептуально?

Бо вона руйнує одразу дві зручні ілюзії. Перша – що витік інформації за допомогою електромагнітного каналу обов'язково потребує дорогого спеціального приймача поряд із жертвою. Друга – що системи – захищені, якщо на самому комп'ютері немає бездротових модулів. Ми показуємо, що кабель може стати передавачем, а навколишня LoRa-інфраструктура – приймачем. Саме ця зв'язка і робить TEMPEST-LoRa новим класом ризику.

Який головний висновок із вашої роботи?

Що електромагнітний канал може бути не лише джерелом пасивного витоку, а й основою для протокольно сумісного бездротового прихованого зв'язку. І якщо цей зв'язок здатен працювати з уже розгорнутими LoRa приймаче/передавачем, то велика відстань між пристрої і мінімально можливим місцем розташування засобу розвідки сама по собі більше не гарантує безпеки так, як звикли думати.

Чому це важливо вже сьогодні

TEMPEST-LoRa важлива не лише як ефектна демонстрація. Вона показує глибшу проблему: сучасне середовище навколо "ізольованого" комп'ютера часто вже насичене сторонньою бездротовою інфраструктурою, яку ніхто не розглядав як напрямок атаки противника. LoRa-шлюз, датчик, індустріальний вузол або просто чужий випромінювач поруч із об'єктом можуть несподівано стати останньою ланкою прихованого каналу витоку. І саме це означає, що тим хто захищає інформацію тепер треба думати не лише про сам пристрій де обробляється інформація, а й через електромагнітну екосистему навколо нього.

Фінальний висновок

Стаття TEMPEST-LoRa: Cross-Technology Covert Communication показує дуже неприємну, але надзвичайно важливу річ: у сучасному технічному світі кабель може стати радіопередавачем, а чужий передавач – мовчазним співучасником витоку. Тут велика відстань вже не виглядає абсолютним захистом, бо сам фізичний тракт виявляється

здатним породити протокольно осмислений бездротовий сигнал. І якщо раніше TEMPEST-канал був переважно проблемою спеціалізованої розвідки, то тепер він дедалі більше стає проблемою звичайної цифрової інфраструктури, яка просто опинилася не в тому місці й не в той час.

Як звичайний диференціальний датчик тиску перетворюється на засіб витоку інформації акустичним канал і дозволяє відновлювати мовну інформацію? [14]

Ми звикли вважати датчики тиску німими елементами інфраструктури. Вони мають стежити за перепадом тиску, підтримувати чисті зони, контролювати систему вентиляції, забезпечувати стабільність у лікарнях, готелях, офісах і напівпровідникових виробництвах. Але стаття A Fly on the Wall – Exploiting Acoustic Side-Channels in Differential Pressure Sensors показує тривожну річ: висока чутливість датчику перепаду тиску робить його не лише інструментом контролю середовища, а й потенційним засобом підслуховування. Якщо поруч із датчиком є гучномовець або просто ведеться розмова між людьми, тонка мембрана датчика може мимоволі вловлювати мікроскопічні коливання повітря. А далі датчик тиску уже починає поводитися як сурогатний мікрофон. Саме на цьому принципі автори будують атаку BaroVox, яка дозволяє частково відновлювати мовну інформацію з показів датчика тиску.

У чому головна ідея вашої роботи?

Ми виявили раніше недооцінену вразливість датчику тиску: через високу чутливість до малих перепадів тиску вони можуть реагувати не лише на повільні зміни середовища, а й на дрібні повітряні вібрації, які створює людський голосовий апарат або техніка для озвучення (колонки, гучномовець). На цій основі ми запропонували атаку BaroVox, яка аналізує покази датчика і намагається відновити зі слабкої зміни тиску корисну мовну інформацію.

Чому це важливо саме зараз?

Тому що такі датчики широко використовуються на об'єктах, де контроль тиску є частиною безпеки або технологічного процесу. При цьому аудіосистеми – інтеркоми, настінні гучномовці, службове озвучення – часто розміщені поруч із такими датчиками. Саме ця близькість і створює акустичний канал витоку.

Тобто датчик фактично стає імпровізованим мікрофоном?

Саме так. У статті ми прямо пишемо, що тонка чутлива мембрана датчика тиску реагує на звукові хвилі, які спричиняють малі коливання повітря. Ці вібрації проходять через елементи датчика і відображаються в показниках тиску. У результаті датчик починає функціонувати як мікрофон, хоча взагалі не призначався для запису звуку.

Який саме фізичний елемент датчика робить це можливим?

Ключову роль відіграє гнучка мембрана. Збирач даних зміни тиску у таких датчиках побудований на тонкому діафрагмовому елементі – наприклад, силіконовій мембрані або подібному матеріалі. Саме ця тонка й еластична структура виявляється достатньо чутливою, щоб уловлювати не лише перепад тиску між двома точками, а й дуже слабкі звукові збурення. Це фундаментальна особливість конструкції, а не випадковий дефект окремої моделі.

Який тип датчика ви використовували в експериментах?

Для демонстрації ми використали термоанемометричний датчик диференціального тиску, зокрема Sensirion SDP800. Але в статті окремо наголошується, що вразливість пов'язана не з конкретним брендом, а з самим механізмом, який є типовим для різних датчиків. Тобто SDP800 тут виступає як приклад, а не єдиний вразливий сенсор.

Чому переговорні у вашій статті займають таке важливе місце?

Тому що переговорні/кабінети для нарад – це дуже показовий приклад середовища, де датчик тиску і звукова система реально співіснують. У переговорних, датчик постійно контролюють перепади тиску, а інтеркоми та настінні гучномовці потрібні для координації персоналу та озвученні інформації на велику кількість осіб. Це робить атаку не академічною фантазією, а реальною загрозою.

Які саме дані можуть витікати через такий канал?

У статті прямо згадуються власна та конфіденційна інформація, параметри процесів, проєктна документація, а також інші конфіденційні розмови в переговорних, корпоративних нарадах, медичних установах або приватних приміщеннях. Тобто йдеться не лише про "чутний шум", а про змістовну мовну інформацію, яка може мати комерційну, технологічну або навіть держану таємницю.

Як виглядає модель атаки у вашій роботі?

Ми припускаємо, що нападник не має фізичного доступу до приміщення і не змінює апаратно сам датчик. Натомість він отримує віддалений доступ до показнику тиску – через скомпрометовану систему моніторингу, зловмисного інсайдера, перехоплення мережевої передачі або доступу до лог-файлів. Це важливо: атака не вимагає приховати окремий мікрофон у кімнаті – достатньо отримати доступ до телеметрії датчика.

Яка головна технічна проблема в такій атаці?

Найбільша складність у тому, що датчик тиску не створювався як аудіосенсор. Його сигнал має низьку смугу, низьке відношення сигнал/шум і нелінійну частотну характеристику. Сенсор значно гірше відтворює високочастотні компоненти мовлення, а після приблизно 0.9 кГц корисна інформація майже зникає. Це робить відновлення мови нетривіальним завданням.

Що ви маєте на увазі під низькою частотою дискредитації?

Для використаного SDP800 теоретична максимальна частота дискретизації становить 2.2 кГц, але фактично корисний аудіодіапазон у наших вимірюваннях закінчувався приблизно на 0.9 кГц. Це набагато менше, ніж потрібно для повноцінного мовлення. У статті прямо зазначено, що така обмеженість призводить до втрати значної частини спектра, потрібного для чіткого сприйняття мови, і суттєво ускладнює атаку.

А що означає нелінійна частотна характеристика в контексті датчика тиску?

Це означає, що датчик не однаково реагує на різні частоти. Автори моделюють датчик тиску як другопорядкову динамічну систему через наявність еластичної діафрагми. З ростом частоти корисний сигнал у відновленому аудіо слабшає, а після певної межі майже тоне в шумі. Отже, відновлений аудіосигнал не є просто "послабленою копією" мови – він частотно спотворений. Саме тому потрібна окрема обробка звуку.

Як саме працює атака BaroVox?

Архітектура атаки починається з перетворення тиску в акустику (PAT), яка перетворює показники тиску у сигнал, ближчий до аудіохвилі. Потім автори пропонують два підходи. Перший – часткова реконструкція мови. Другий – автоматичне розпізнавання слів із обмеженого словника.

Чому ви розділили рішення на два напрями?

Бо вони розв'язують різні атакувальні задачі. Перший орієнтований на покращення якості відновленого аудіо, так, щоб людина могла частково зрозуміти розмову. Другий орієнтований на більш точне автоматичне виявлення конкретних ключових слів, команд або чисел із заданого словника. Перший шлях гнучкіший щодо лексики, другий – ефективніший, коли нападника цікавлять конкретні критичні слова.

Що нового у вашому рішенні?

Одним із ключових внесків є спеціальна схема на основі алгоритму цифрової обробки сигналів для зменшення фонового шуму в аудіо. Ми не просто віднімаємо шум, а спочатку розділяємо сигнал на гармоніки і ударні компоненти через медіанний фільтр. Далі для них застосовується різний рівень шумопригнічення, щоб зменшити шум, але не зруйнувати важливі елементи мовлення. Додатково використовується фільтр на 40 Гц і метод обробки сигналів (FDE), який компенсує нерівномірну частотну характеристику.

Наскільки сильним було покращення після обробки?

У статті наведені конкретні приклади. Фільтр підвищує SNR для тестового запису з 7.464 дБ до 8.888 дБ, спектральне віднімання дає подальший приріст до 9.921 дБ, а метод FDE піднімає SNR до 15.382 дБ. Тобто мова не стає "ідеальною", але поступово переходить із майже нерозбірливого тискового сигналу в форму, де суттєва частина змісту вже відновлюється.

Яких результатів ви досягли для ручного розпізнавання мовлення?

Для ручного розпізнавання мови автори залучили 18 добровольців, які транскрибували реконструйовану мову. У середньому для звичайної розмови отримано WER 0.35 і MOS 4.09/5. Для закритих фраз результати були нижчими без контексту, але після короткого введення в контекст розмови середній WER знизився до 0.29, а MOS виріс до 3.71/5. Це означає, що людина може відновити понад 70% змісту навіть із такого нетипового джерела, як сенсор тиску.

А як працює ваш автоматичний варіант?

У другому варіанті ми використовуємо модель глибокого навчання, яка об'єднує дві функції: автоматичне розпізнавання мовлення (ASR) та подальшу класифікацію отриманих результатів на основі ResNet (нейронної мережі). Для перевірки обрано обмежений словник – передусім спеціалізований оператор та синтаксис з набору SpeechCommands. Це відображає реальні сценарії, де нападника можуть цікавити короткі інструкції, числа, параметри або ключові слова. У статті пояснюється, що дані оригінального датасету перетворюються через акустично-тискову трансформацію в структурований масив інформації, який містить записи коливань, на якому вже навчається модель.

Яку точність показало автоматичне розпізнавання?

Найкраща модель досягла 90.51% відтворення на словника з 35-ти ключових термінів. Для статті такого типу це дуже сильний результат, бо йдеться не про

мікрофонні записи, а про низькосмугові, зашумлені сигнали. Автори окремо підкреслюють, що додавання спеціальних шумоподавлення та регулювання гучності дало помітний приріст відносно базового ResNet.

Чи означає це, що BaroVox вже є практично небезпечним?

Так. І саме це є головним висновком статті. Автори прямо наголошують, що навіть часткова реконструкція мови з датчику тиску має серйозні наслідки. Для більшості компаній чи державних установ цього вже достатньо, щоб витягати конфіденційну, технологічну та іншу інформацію. Це не ідеальний запис розмови, але вже цілком працездатний канал витоку мовної інформації.

Який головний висновок із вашої роботи?

Що датчик диференціального перепаду тиску не можна більше розглядати лише як нейтральні елементи приміщення. Вони здатні стати ненавмисними слухачами середовища. BaroVox показує, що навіть не аудіосенсор, якщо він достатньо чутливий і правильно розміщений, може перетворитися на канал витоку мовної інформації. А отже при захисті інформації, що озвучується в приміщені тепер брати до уваги не лише наявні мережі, мікрофони чи лазерні системи, а звичайні датчики тиску.

Чому це важливо вже сьогодні

BaroVox небезпечний саме тим, що атакує не екзотичний пристрій, а повсякденний елемент інженерної інфраструктури. Датчики тиску встановлюють для безпеки, контролю чистоти, управління повітряними потоками та підтримки режимів приміщення. Ніхто не сприймає їх як акустичні сенсори. Саме тому вони ідеально вписуються в сучасну логіку загрози безпеки інформації: найбільш цікаві витоки часто з'являються не там, де є спеціалізований канал запису, а там, де високочутливий технічний вузол випадково починає чути більше, ніж йому належить.

Фінальний висновок

Стаття A Fly on the Wall – Exploiting Acoustic Side-Channels in Differential Pressure Sensors показує дуже неприємну істину сучасної технічної безпеки: іноді підслуховує не той пристрій, який створили для цього, а той, якому просто дали достатньо чутливу мембрану і поставили його не в тому місці. Датчик тиску у цій роботі перетворюється з інструмента контролю середовища на побічний канал витоку інформації. І саме тому справжній захист приміщення сьогодні починається не лише з контролю мікрофонів і мережевих інтерфейсів, а з розуміння того, які інженерні сенсори поруч із нами вже мимоволі стали “мухою на стіні”.

Як сучасне глибоке навчання перетворює звук натискань на практичний канал витоку навіть через смартфон і Zoom [15]

Ми звикли думати, що клавіатура видає інформацію лише на екран. Але кожне натискання має ще один вихід – звук. Тихий, звичний, майже побутовий. Саме тому він і небезпечний: люди рідко сприймають акустику клавіатури як серйозний канал витоку. Стаття A Practical Deep Learning-Based Acoustic Side Channel Attack on Keyboards показує, що це вже помилка. Автори демонструють повністю автоматизовану атаку, в якій звуки натискань із ноутбука аналізуються сучасною моделлю Deep Learning (нейронна мережа), а далі перетворюються масив даних конкретних клавіш. І найтривожніше тут не лише висока точність, а й практичність: для атаки достатньо звичайного смартфона поруч або навіть аудіо з Zoom-дзвінка.

У чому головна ідея вашої роботи?

Ми хотіли показати, що витік інформації за рахунок аналізу звук з клавіатуру вже не є лабораторною екзотикою. У роботі ми побудували практичну, повністю автоматизовану технологію перехоплення даних, яка включає ізоляцію окремих натискань, виділення ознак і класифікацію клавіш за допомогою сучасної deep learning моделі. Головний результат полягає в тому, що навіть із використанням звичайного обладнання можна досягати дуже високої точності.

Чому ця проблема стала такою актуальною саме тепер?

Тому що збіглися три фактори. По-перше, мікрофони сьогодні всюди: у смартфонах, ноутбуках, вебкамерах, системах VoIP, смартпристроях. По-друге, сучасні онлайн-сервіси, особливо відеоконференції, постійно передають аудіо назовні. По-третє, deep learning моделі суттєво посилили здатність виділяти тонкі патерни зі складних даних. У статті прямо підкреслюється, що зростання якості мікрофонів і доступності спеціалізовних інструментів різко підвищило практичність таких атак.

Але клавіатури сьогодні значно тихіші, ніж старі механічні. Хіба це не зменшує ризик?

Частково так, але не настільки, як можна було б сподіватися. Автори прямо зазначають, що сучасні ноутбуки, особливо тонкі моделі, дійсно мають менш виражену акустику, ніж старі товсті або механічні клавіатури. Однак водночас значно покращилися засоби запису та обробки сигналу. У підсумку тихіша клавіатура вже не означає безпечну клавіатуру.

Чому ви зосередилися саме на ноутбуках?

Тому що ноутбуки є особливо реалістичною мішенню. Вони мобільні, часто використовуються в публічних або напівпублічних просторах, а ще багато моделей мають дуже подібні клавіатури. У статті наголошується, що немодульність ноутбуків і повторюваність дизайну клавіатур всередині популярних лінійок роблять успішну атаку масштабованою: якщо одна модель виявляється вразливою, ризику піддається велика група користувачів.

Який головний технічний внесок вашої роботи?

Ми вперше для такої задачі використали deep learning модель, тобто архітектуру, що спирається на сучасну логіку attention-based processing(технологія штучного інтелекту, яка імітує людську здатність фокусуватися). Автори обрали CoAtNet, яка поєднує локальний та глобальний аналізи. Саме це дозволило побудувати класифікатор, який працює не просто з грубими статистичними ознаками, а з тонкою структурою аудіосигналу, поданою у вигляді візуальних ознак.

Чому ви взагалі подаєте звук як зображення?

Бо ми працюємо не з сірим сигналом напряму, а з мел-спектрограмами. Це один із ключових інженерних виборів статті. Мел-спектрограма перетворює звук на двовимірне представлення, де по одній осі час, по іншій – частота, а яскравість відображає амплітуду. Такі представлення виявилися добре сумісними з deep learning моделями. Автори пояснюють, що мел-спектрограма краще відображає важливі низькочастотні компоненти клавішних звуків, ніж лінійний FFT-підхід.

Як виглядає повний конвеєр атаки?

Спершу з довгого запису потрібно ізолювати окремі натискання клавіш. Для цього використовується сегментація на основі енергії: сигнал перетворюється через FFT, енергія сумується по частотах, а потім за порогом визначаються моменти натискань. Далі кожне натискання обрізається до фіксованого фрагмента, проходить через аугментацію, перетворюється в мел-спектрограму і подається в deep learning класифікатор.

Чому це настільки важливо?

Тому що саме тут атака переходить із локального сценарію в реально віддалений. У статті прямо ставиться питання: чи можлива атака через VoIP з урахуванням компресії та втрати інформації в аудіоканалі. І відповідь – так. Zoom-записи, попри шумозаглушення і втрати, усе одно містять достатньо інформації для успішної класифікації натискань. Це означає, що атака не вимагає обов'язкової фізичної присутності поряд із жертвою.

Які саме сценарії ви перевіряли?

Два головні. Перший – відновлення за допомогою телефону, коли iPhone 13 mini розміщений приблизно за 17 см від MacBook. Другий – відновлення за допомогою Zoom, коли натискання захоплюються через вбудований мікрофон ноутбука і записуються в межах Zoom-сесії. Саме порівняння цих двох сценаріїв дає роботі особливу практичну вагу: один показує локальну атаку поруч із жертвою, інший – повністю віддалений сценарій.

Наскільки високої точності ви досягли?

Для відновлення з телефоном автори отримали 95% точності, що прямо названо найвищим результатом без використання мовної моделі. Для відновлення через Zoom точність становила 93%, і це подано як новий рівень для цього каналу. Це вже справді виглядає небезпечно.

Але чи не потрібні для цього великі обсяги даних?

Дані потрібні, але не астрономічні. У роботі використано 36 клавіш – 0–9 і a–z – кожну натискали 25 разів поспіль. Тобто йдеться не про мільйони прикладів, а про доволі досяжний датасет. Автори також використовували сучасні техніки для збільшення обсягу та різноманітності навчальної вибірки Це допомагає моделі узагальнювати й зменшує потребу в надто великих обсягах сирих записів.

Чому саме CoAtNet виявився вдалим вибором?

Тому що він поєднує дві сильні сторони: локальний аналіз для швидкого виділення локальних патернів і глобальний для оцінки важливості цих патернів у ширшому контексті. Для мел-спектограми це особливо корисно, бо звук натискання клавіш має і локальні, і структурні особливості. Автори прямо пояснюють, що така комбінація дала можливість краще працювати з візуально репрезентованими акустичними даними, ніж з іншими більш старілими підходами.

А як поводилися помилки моделі? Вони були випадковими?

Ні, і це дуже цікаво. Автори звернули увагу, що хибні класифікації часто групуються поблизу справжньої клавіші. У матриці помилок видно, що багато з них припадають на сусідні або близькі клавіші. Це означає, що навіть коли модель не вгадує точну літеру, вона нерідко все одно відновлює позиційну інформацію про натискання. А така помилка може бути дуже корисною для подальших атак або мовних моделей.

Чи використовували ви мовну модель для покращення результату?

Ні, і це один із важливих моментів. Автори окремо підкреслюють, що 95% для смартфонного запису досягнуто без мовної моделі. Це важливо, бо показує: навіть сам по собі акустичний класифікатор уже дуже

сильний. А якщо в майбутньому додати мовну модель, словникові обмеження або контекстний постпроцесинг, результат може стати ще небезпечнішим.

Які захисти ви вважаєте реалістичними?

У статті обговорюється кілька напрямів. По-перше, зміна стилю друку може ускладнювати атаку. По-друге, складні й рандомізовані паролі з кількома регістрами зменшують користь від часткового відновлення. По-третє, для VoIP-сценаріїв перспективним є автоматичне придушення або маскування звуків натискань у самих комунікаційних платформах. По-четверте, зниження ризику дає двохфакторна автентифікація та біометрія, бо вони зменшують залежність від набору паролів на клавіатурі. Автори прямо зазначають, що фейкові натискання клавіатури додані можуть бути ефективнішими за звичайний білий шум.

Який головний висновок із вашої роботи?

Що акустична атака на клавіатуру вже є практичною, автоматизованою і високоточною навіть на сучасних ноутбуках і навіть через віддалений аудіоканал на кшталт Zoom. Це означає, що клавіатурний звук більше не можна вважати нешкідливим побутовим фоном. У поєднанні з сучасними deep learning моделями він стає повноцінним каналом витоку інформації.

Чому це важливо вже сьогодні

У цієї роботи є одна особливо неприємна риса: вона не спирається на спеціальну апаратуру. Її сила саме в буденності. Смартфон на столі, ноутбук із мікрофоном, Zoom-дзвінок, звичайна тиха клавіатура – усе це давно стало нормальним фоном сучасної роботи. І саме цей фон виявляється достатнім, щоб побудувати практичний канал витоку. Коли атака працює на звичайному обладнанні, межа між академічною демонстрацією і реальною загрозою стає дуже тонкою.

Фінальний висновок

Стаття A Practical Deep Learning-Based Acoustic Side Channel Attack on Keyboards показує сучасну правду про безпеку: інколи найбільша загроза приходить не з нової апаратури, а зі звичайних речей, які вже лежать поруч із нами. Клавіатура стукає, мікрофон слухає, алгоритм навчається – і цього виявляється достатньо, щоб звук натискань перетворився на текстовий слід. У світі, де штучний інтелект дедалі краще витягає структуру з шуму, справжній захист починається не з ігнорування побічних сигналів, а з визнання того, що навіть найзвичніший звук може виявитися мовою витоку.

Перелік джерел посилання

1. Fernández S., Martínez E., Varela G., Musé P., Larroca F. Deep-TEMPEST: Using Deep Learning to Eavesdrop on HDMI from its Unintended Electromagnetic Emanations. Proceedings of Submitted. New York, NY : ACM, 2024. 10 p. DOI: 10.48550/arXiv.2407.09717
2. Long Y., Jiang Q., Yan C., Alam T., Ji X., Xu W., Fu K. EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Camera. Network and Distributed System Security (NDSS) Symposium 2024. San Diego, CA, USA, 2024. DOI: 10.14722/ndss.2024.24552
3. Sayakkara A. P. Electromagnetic Side-Channel Analysis Methods for Digital Forensics on Internet of Things : PhD thesis. Dublin : University College Dublin, School of Computer Science, 2020. 194 p. https://markscanlon.co/papers/PhDThesis-ElectromagneticSideChannelAnalysisMethodsIoT.pdf
4. Loughry J. Optical TEMPEST. arXiv. 2018. DOI: 10.48550/arXiv.1808.07175
5. Popp A., Sedlmeir F., Stiller B., Marquardt C. Eavesdropper localization for quantum and classical channels via nonlinear scattering. Optica Quantum. 2024. Vol. 2, No. 1. Article 21. DOI: 10.1364/OPTICAQ.502944
6. Wang C., Zhou X., Zhang C., Ji H., Qiu J. Research on Active Interference Technology Based on Piezoelectric Flexible Structure. Actuators. 2026. Vol. 15, No. 1. Article 62. DOI: 10.3390/act15010062
7. Sydorkin P., Nesterenko S., Salnyk S., Konotopets M., Kulynich O., Smolkov O. Methods and techniques of protecting information from leakage by technical channels via side electromagnetic radiation. Political Science and Security Studies Journal. 2021. Vol. 2, No. 3. P. 15–25. DOI: 10.5281/zenodo.5534847
8. Woo J., Ryu D., Seo D., Kim Y.-S., Lee N., Cassuto Y., Kim Y. Mutual Information Minimization for Side-Channel Attack Resistance via Optimal Noise Injection. arXiv. 2025. DOI: 10.48550/arXiv.2504.20556
9. Bari M. F., Xie Y., Choudhury M. R., Sen S. Keystroke Detection by Exploiting Unintended RF Emission from Repaired USB Keyboards. arXiv. 2025. DOI: 10.48550/arXiv.2509.00043
10. Liu G., Chen G., Liu W. The Inevitability of Side-Channel Leakage in Encrypted Traffic. arXiv. 2026. DOI: 10.48550/arXiv.2602.14055
11. Hu B. Reconstruction of Video Electromagnetic Leakage from Computer. Modern Applied Science. 2007. Vol. 1, No. 2. P. 56. DOI: 10.5539/mas.v1n2p56
12. Pavlenko Y. Determination of signal level for protection of information in case of its interception by technical means of intelligence. Technology Audit and Production Reserves. 2023. Vol. 4, No. 1(72). P. 25–28. DOI: 10.15587/2706-5448.2023.286193
13. Sun X., Zheng Y., Xi W., Chen Z., Chen Z., Hao H., Jiang Z., Zhong S. TEMPEST-LoRa: Cross-Technology Covert Communication. Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security. 2025. P. 678–692. DOI: 10.1145/3719027.3744817
14. Achamyeleh Y. G., Fakih M. H., Garcia G., Barua A., Al Faruque M. A. A Fly on the Wall — Exploiting Acoustic Side-Channels in Differential Pressure Sensors. 2024 Annual Computer Security Applications Conference (ACSAC). Honolulu, HI, USA, 2024. P. 240–256. DOI: 10.1109/ACSAC63791.2024.00034
15. Harrison J., Toreini E., Mehrnezhad M. A Practical Deep Learning-Based Acoustic Side Channel Attack on Keyboards. arXiv. 2023. DOI: 10.48550/arXiv.2308.01074

Сучасні наукові дослідження та тенденції розвитку ТЗІ



Аналіз сучасних наукових досліджень та публікацій у сфері технічного захисту інформації

д-р філософії Іван ЦМОКАНИЧ, ДержНДІ технологій кібербезпеки
Дмитро МОНАХОВ, ДержНДІ технологій кібербезпеки

Акустичні канали витоку інформації під час натискання клавіш клавіатури [1]

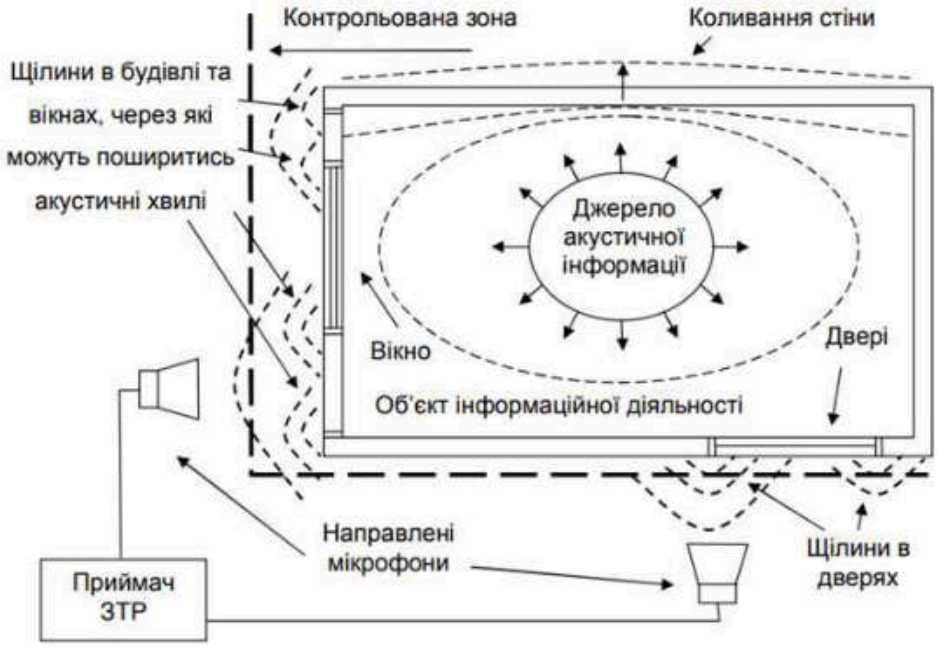
Одним із перспективних напрямів дослідження побічних каналів витоку інформації є **аналіз фізичних проявів роботи комп'ютерних засобів**, які можуть ненавмисно **розкривати оброблювані дані**. Особливу увагу в цьому контексті привертають **акустичні сигнали**, що виникають під час функціонування периферійних пристроїв і можуть бути використані для **відновлення конфіденційної інформації**. Цікаві результати за цим питанням представлені в статті "Acoustic Side-Channel Vulnerabilities in Keyboard Input Explored Through Convolutional Neural Network Modeling: A Pilot Study" авторів Michal Rzemieniuk, Artur Niewiarowski та Wojciech Ksiazek з Краківської політехніки імені Тадеуша Костюшка (Польща).



Зображення створено за допомогою ШІ

У даній роботі представлено результати дослідження, присвяченого **аналізу акустичних каналів витоку інформації**, що виникають під час **введення даних з клавіатури**. Проведений аналіз спрямований на вивчення можливості відновлення текстової інформації на основі звукових сигналів, які утворюються під час натискання клавіш.

Акустичний канал витоку інформації



ela.kpi.ua/server/api/core/bitstreams/930d9270-2cb1-4c62-a4ce-ab5404d9b90f/content

Автори розглядають акустичні сигнали як побічні фізичні прояви функціонування комп'ютерної периферії, що можуть містити значну кількість інформативних характеристик.

> Основа дослідження

Основою дослідження стала **побудова експериментального середовища для реєстрації звукових сигналів клавіатури** з подальшим застосуванням алгоритмів глибинного навчання для класифікації отриманих акустичних шаблонів.

У процесі дослідження було сформовано **спеціалізований набір даних**, що складався з великої кількості аудіозаписів натискань клавіш. Для подальшого аналізу ці записи піддавалися попередній обробці з використанням методів цифрової обробки сигналів, включаючи перетворення Фур'є, фільтрацію шумів та побудову мел-спектрограм. Такі представлення сигналів дозволили виділити спектральні характеристики, які відображають особливості акустичних коливань, спричинених механічним контактом клавіш із корпусом клавіатури. Отримані спектральні ознаки використовувалися як вхідні дані для згорткових нейронних мереж, здатних виконувати автоматичне виділення релевантних характеристик та їх класифікацію. Результати експериментів засвідчили, що навіть у відносно шумному середовищі можливо досягти значного рівня точності ідентифікації натискань клавіш на основі акустичних сигналів.

Нейронна мережа змогла навчитися розрізняти акустичні патерни окремих клавіш, що підтверджує наявність стабільних акустичних характеристик для кожного елемента клавіатури. Таким чином було продемонстровано можливість реконструкції текстової інформації на основі аналізу звукових коливань.

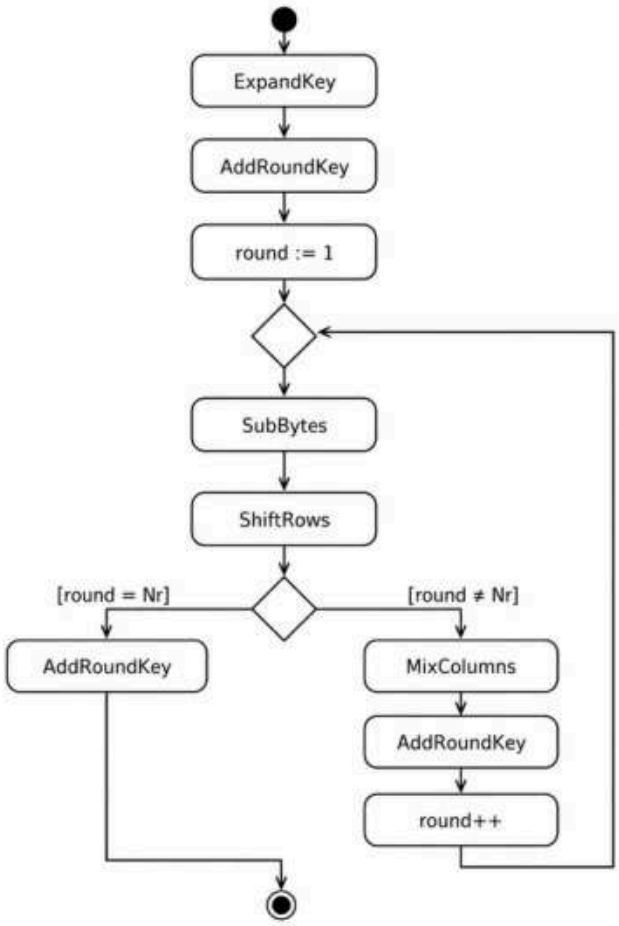
Результати дослідження

Отримані результати мають важливе значення для галузі технічного захисту інформації, оскільки підтверджують існування реального ризику витоку даних через акустичні побічні випромінювання комп'ютерної техніки та підкреслюють необхідність розроблення спеціалізованих засобів захисту від подібних атак.

Сучасні методи аналізу побічних каналів, що застосовуються для атак на криптографічні реалізації алгоритму AES [2]

Оскільки більшість сучасних атак побічними каналами націлені на реалізації алгоритму **AES**, важливим є розуміння структури його процесу шифрування та внутрішніх перетворень, під час виконання яких можуть виникати інформативні фізичні витоки. Особливий інтерес для дослідників становлять проміжні значення, що формуються на окремих етапах алгоритму, насамперед під час операцій SubBytes та AddRoundKey, оскільки саме вони часто корелюють із параметрами енергоспоживання або електромагнітного випромінювання пристрою. Загальну послідовність раундів і базових перетворень алгоритму AES наведено на рисунку нижче.

Алгоритм шифрування AES



> Акцент роботи Робота зосереджена на використанні **алгоритмів глибинного навчання для автоматизованого аналізу фізичних сигналів**, які виникають під час виконання криптографічних операцій.

У традиційних методах криптоаналізу побічних каналів аналіз ґрунтувався на статистичних методах, таких як диференційний аналіз споживання енергії або кореляційний аналіз електромагнітних випромінювань. Однак у сучасних дослідженнях дедалі ширше використовуються нейронні мережі, здатні автоматично виявляти складні залежності між фізичними сигналами та оброблюваними даними.

У дослідженні розглядається **процес збору великої кількості трас електромагнітних або енергетичних сигналів**, що генеруються криптографічними пристроями під час виконання операцій шифрування. Ці сигнали містять інформацію про проміжні значення алгоритму, які можуть бути використані для відновлення секретного ключа. Для аналізу отриманих сигналів застосовуються **згорткові** та **рекурентні нейронні мережі**, що дозволяють виконувати автоматичне виділення характерних патернів без необхідності ручного визначення статистичних ознак.

На відміну від класичних підходів, які потребують попереднього вибору інформативних ділянок сигналу та ручного формування статистичних ознак, моделі глибинного навчання навчаються безпосередньо на отриманих трасах побічних випромінювань. Це дозволяє автоматично встановлювати зв'язок між характеристиками фізичного сигналу та проміжними станами алгоритму AES, що виникають під час оброблення даних. Такий підхід суттєво спрощує процес аналізу та забезпечує можливість ефективного відновлення інформації навіть у випадках наявності шумів, маскування або інших захисних механізмів.

Результати дослідження

Отримані результати демонструють високу ефективність підходу, заснованого на глибинному навчанні, у задачах відновлення секретних ключів. **Нейронні мережі здатні аналізувати складні нелінійні залежності між параметрами сигналу та внутрішніми станами криптографічного алгоритму**, що значно підвищує результативність атак побічних каналів. У контексті технічного захисту інформації ці результати підкреслюють необхідність розроблення нових методів апаратного та програмного захисту криптографічних пристроїв, які повинні враховувати можливості сучасних алгоритмів машинного навчання.

Витік інформації через електромагнітні випромінювання сенсорних екранів [3]

У статті “Capacitive Touchscreens at Risk: Recovering Handwritten Trajectory on Smartphone via Electromagnetic Emanations” досліджується проблема витоку інформації через електромагнітні побічні випромінювання сенсорних екранів мобільних пристроїв.

Сенсорні екрани мобільних пристроїв



Автори роботи розглядають можливість відновлення рукописних траєкторій, що вводяться користувачем на екрані смартфона, на основі аналізу **електромагнітних сигналів**, які генеруються під час взаємодії пальця користувача з сенсорною поверхнею.

У дослідженні представлено методологію неінвазивного перехоплення електромагнітних сигналів, що виникають у процесі роботи ємнісних сенсорних панелей. В основі методу лежить припущення, що **зміни електричного поля**, спричинені переміщенням пальця користувача по поверхні екрана, призводять до появи характерних **електромагнітних коливань**, які можуть бути зафіксовані спеціалізованими вимірювальними пристроями. Для перехоплення таких сигналів використовувалися високочутливі антени та спектральні аналізатори, що дозволяють реєструвати слабкі електромагнітні випромінювання в широкому частотному діапазоні.

Після реєстрації сигналів здійснювалася їх цифрова обробка з

використанням алгоритмів машинного навчання, спрямованих на реконструкцію двовимірної траєкторії руху пальця. Для цього застосовувалися моделі регресійного аналізу, здатні перетворювати часові ряди електромагнітних сигналів у координатні дані, що відображають рух користувача по поверхні екрана. Результати експериментів показали, що запропонований підхід дозволяє з високою точністю відновлювати форму написаних символів і навіть виконувати їх подальше розпізнавання.

Результати дослідження

Отримані результати демонструють, що електромагнітні випромінювання сенсорних екранів можуть становити потенційний канал витоку конфіденційної інформації, зокрема під час введення паролів або інших секретних даних.

Акустичні побічні сигналів для забезпечення безпеки промислових роботизованих систем [4]

У статті "ASIDS: Acoustic Side-Channel Based Intrusion Detection System for Industrial Robotic Arms" розглядається застосування акустичних побічних сигналів для забезпечення безпеки промислових **роботизованих систем**. Дослідження зосереджене на створенні системи виявлення вторгнень, яка використовує акустичні характеристики роботи **роботизованих маніпуляторів** для ідентифікації аномальних режимів функціонування.

Роботизовані маніпулятори



Промислові роботи широко використовуються у виробничих процесах, і їх робота супроводжується характерними акустичними сигналами, які формуються внаслідок руху механічних компонентів, роботи електродвигунів і передач. Автори дослідження виходять з припущення, що кожна

траєкторія руху роботизованої руки відповідає певному акустичному профілю. У разі зміни програмного керування або несанкціонованого втручання у роботу системи ці акустичні характеристики також змінюються.

Для перевірки цієї гіпотези було проведено експериментальне дослідження, у межах якого здійснювалася реєстрація **акустичних сигналів**, що генеруються **роботизованими маніпуляторами** під час виконання різних виробничих операцій. Отримані сигнали піддавалися аналізу з використанням алгоритмів машинного навчання, здатних класифікувати нормальні та аномальні режими роботи системи. Результати дослідження показали, що акустичний аналіз дозволяє з високою точністю виявляти відхилення у поведінці роботизованих систем, що може свідчити про несанкціоноване втручання або помилки в програмному забезпеченні.

Таким чином, запропонований підхід відкриває нові можливості для використання побічних фізичних сигналів як інструменту забезпечення безпеки промислових інформаційно-керуючих систем.

Методи підвищення ефективності екранування ПЕМВН електронної техніки [5]

Питання протидії витоку інформації через побічні електромагнітні випромінювання та наведення залишаються одним із ключових напрямів досліджень у сфері технічного захисту інформації. Значний внесок у розвиток цього напряму здійснюють вітчизняні науковці, результати робіт яких регулярно публікуються у спеціалізованих фахових виданнях. Зокрема, актуальні дослідження з проблем екранування електронної техніки, зниження рівня ПЕМВН та підвищення захищеності технічних засобів обробки інформації висвітлюються на сторінках науково-технічного журналу «Озброєння та військова техніка», який є одним із провідних українських наукових видань у галузі оборонних технологій та технічного захисту інформації.

> Новизна

Даною статтею було вперше в українській науковій літературі системно проаналізовано та запропоновано комплекс нових композитних матеріалів і технологій, які дозволяють кардинально підвищити ефективність захисту електронної техніки від витоку інформації по каналах **побічних електромагнітних випромінювань і наведень (ПЕМВН).**



Автори (Олександр Ковбасюк, Олександр Башкиров, Олександр Ковалько та Сергій Ступак), працюючи в Центральному науково-дослідному інституті озброєння та військової техніки Збройних Сил України, розглянули фізичні механізми виникнення компрометуючих випромінювань у сучасній комп'ютерній та телекомунікаційній апаратурі – від гармонік тактових сигналів процесорів і відеокарт до наведень на інтерфейсних кабелях HDMI, USB, SATA та живлення, – і довели, що традиційні металеві екрани та сітки вже недостатньо ефективні проти високошвидкісних цифрових сигналів 5G/6G-рівня та side-channel атак з використанням машинного навчання.

У статті детально обґрунтовано перехід до багатофункціональних полімерних композитів, наповнених графеном, вуглецевими нанотрубками, наночастинками срібла та феритами, які забезпечують одночасно високе поглинання (до 45–60 дБ у діапазоні 100 МГц – 10 ГГц) і відбиття електромагнітних хвиль, при цьому зберігаючи малу масу та гнучкість для нанесення на корпуси, кабелі та внутрішні плати. Особлива увага приділена гібридним наноструктурним покриттям на основі поліаніліну та поліпіролу з включенням

метаматеріалів, які створюють «невидимий» ефект поглинання за рахунок негативної діелектричної проникності, що дозволяє зменшити рівень **ПЕМВН** від периферійних пристроїв (клавіатури, миші, монітори) на 25–35 дБ порівняно зі стандартними екранами. Автори провели розрахунково-експериментальне моделювання в програмних пакетах CST Studio та Ansys HFSS, підтвердивши, що застосування запропонованих матеріалів у TEMPEST-сумісних конструкціях знижує радіус небезпечної зони витоку інформації з 5–7 метрів до менше 1 метра навіть при максимальному навантаженні процесора.

Ключовим практичним **результатом роботи** є рекомендації щодо інтеграції цих матеріалів у комплекси технічного захисту інформації: обов'язкове використання гнучких екранованих кабелів з новим композитним заповнювачем, нанесення тонкоплівкових покриттів на корпусні деталі серверів і робочих станцій, а також комбінування пасивного екранування з активним зашумленням генераторами шуму нового покоління. Автори показали, що такі рішення повністю відповідають вимогам сучасних методик оцінки захищеності об'єктів інформаційної діяльності, дозволяють проходити атестацію за оновленими нормами ПЕМВН без значного збільшення вартості та масогабаритів обладнання. У висновках підкреслено, що впровадження запропонованих технологій дає змогу Україні перейти на новий рівень протидії технічним розвідкам, особливо в умовах зростання загроз від Deep-TEMPEST-атак і акустико-електромагнітних комбінованих каналів витоку.

На сьогодні, у березні 2026 року, ця стаття є найактуальнішим науковим джерелом для фахівців технічного захисту інформації: її рекомендації вже враховуються при оновленні стандартів **НД ТЗІ**, розробленні **профілів безпеки** для державних об'єктів та виборі матеріалів для паспортизації комплексів захисту. Робота безпосередньо впливає на практику атестації, оскільки надає конкретні кількісні показники підвищення ефективності екранування, які можуть бути використані при розрахунку зон безпеки та виборі засобів протидії **ПЕМВН** для накопичувачів, периферії та кабельних систем. Стаття оприлюднена у відкритому доступі на сайті журналу Центрального науково-дослідного інституту озброєння та військової техніки та на ResearchGate, що робить її обов'язковою для вивчення всіма, хто займається екрануванням, паспортизацією комплексів ТЗІ та протидією технічним каналам витоку інформації в Україні. Саме завдяки таким дослідженням сфера технічного захисту інформації отримує реальні інструменти для протистояння сучасним загрозам, забезпечуючи найвищий рівень захищеності службової інформації та державної таємниці від несанкціонованого перехоплення по електромагнітних і наведених каналах.

Ефективний захист 3D-принтерів від акустичних side-channel атак шляхом модифікації G-code [6]

Дослідженням авторів SAG Asgar та колег "QuietPrint: Protecting 3D Printers Against Acoustic Side-Channel Attacks", опублікованим на arXiv 2 лютого 2026 року, було вперше запропоновано інноваційний метод захисту інтелектуальної власності в адитивному виробництві від крадіжки через акустичні побічні канали, що базується на мінімальних модифікаціях G-code без компрометації якості друку.

Автори детально проаналізували **фізичні механізми акустичного витоку**: вібрації крокових двигунів, шум екструдера та рух осей, які генерують характерні звукові сигнатури, дозволяючи відновлювати траєкторію друку та параметри моделі (наприклад, швидкість, інфіл, шар товщини) з точністю до 90% за допомогою смартфона на відстані понад 10 м. Метод QuietPrint інтегрує алгоритм випадкового пертурбації G-code, додаючи шумові команди (наприклад, мікро-зміщення осей або варіації швидкості) для маскування акустичних патернів, при цьому зберігаючи ефективність друку з додатковими витратами часу менше 5% і без впливу на структурну цілісність об'єкта. Експерименти на стандартних FDM-принтерах (наприклад, Prusa i3) з використанням градієнтних бустованих дерев рішень для атаки та оборонних заходів продемонстрували зниження точності відновлення IP з 85% до менше 10%, що робить цей підхід практичним для захисту конфіденційних прототипів у промисловості.

3D принтер



На сьогодні, у березні 2026 року, це дослідження є ключовим трендом у сфері технічного захисту інформації, оскільки акустичні side-channel атаки на 3D-принтери еволюціонували з теоретичних (як у роботах 2016–2024 років про відновлення G-code через звук) до реальних загроз, особливо в air-gapped системах, де друк медичних імплантатів чи військових компонентів вимагає посиленого зашумлення.

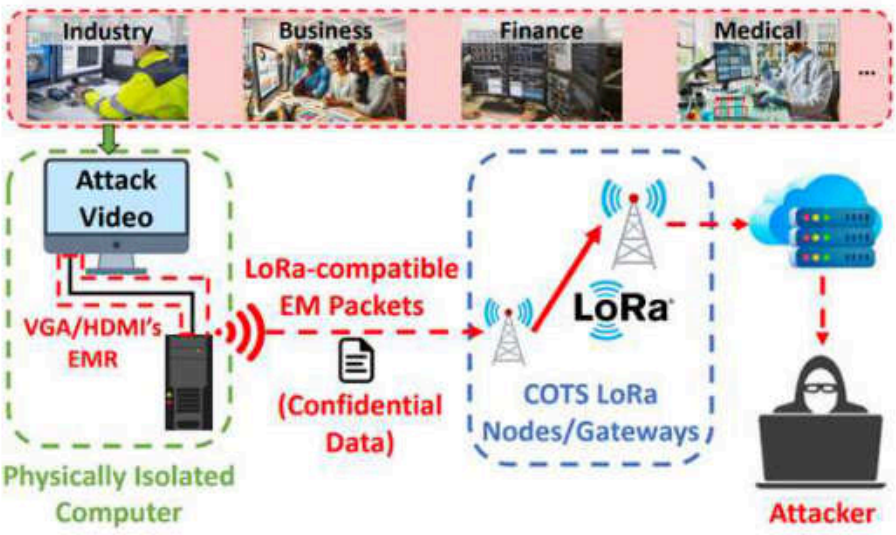
> Відповідність

Робота повністю відповідає стандартам NATO щодо TEMPEST і НД ТЗІ, пропонуючи інтеграцію в slicer-програми (наприклад, Cura або PrusaSlicer) для автоматичного захисту, і її висновки вже впливають на оновлення профілів безпеки для об'єктів інформаційної діяльності, де проводиться 3D-друк з обмеженим доступом.

Дослідження оприлюднене у відкритому доступі на arXiv та Semantics Scholar, слугуючи базою для подальших розробок у комбінованому захисті від акустичних і магнітних каналів витоку.

Створення прихованого каналу витоку даних з air-gapped систем через компрометуючі випромінювання кабелів [7]

Дослідженням авторів Xieyang Sun та колег "TEMPEST-LoRa: Cross-Technology Covert Communication", представленим на ACM CCS 2025 та опублікованим на arXiv 26 червня 2025 року, було розкрито нову вразливість у формі крос-технологічного прихованого каналу витоку даних з air-gapped систем через маніпуляцію електромагнітними випромінюваннями (EM) від відеокабелів (VGA або HDMI), що генерують сумісні з LoRa пакети для передачі секретної інформації на відстані до 87,5 м.



TEMPEST-LoRa демонструє нову приховану міжтехнологічну атаку: через маніпуляції відеокабелями генеруються EM-пакети, сумісні з LoRa, які приймаються існуючими LoRa-вузлами/шлюзами

Автори детально описали фізичні механізми: malware на ізольованому комп'ютері генерує спеціальні піксельні патерни, які викликають гармоніки в кабелі, модулюючи EM-випромінювання на частотах ISM-діапазону (868–915 МГц) з параметрами LoRa (SF 7–12, BW 125–500 кГц), дозволяючи приймати дані стандартними COTS LoRa-приймачами (наприклад, Semtech SX1276) навіть через бетонні стіни товщиною до 20 см. Експерименти з використанням SDR (HackRF One) для емуляції та реальних LoRa-шлюзів продемонстрували швидкість передачі до 21,6 кбіт/с на 40 м з антеною високого посилення та можливість прихованого режиму (екран вимкнено), з BER менше 10↓4 за умови оптимальної модуляції. Підхід TEMPEST-LoRa розширює класичні TEMPEST-атаки, додаючи крос-технологічну сумісність, що робить його загрозою для високозахищених мереж, де традиційні EM-канали обмежені відстанню.

> Актуальність

На сьогодні, у березні 2026 року, це дослідження є актуальним трендом у **протидії технічним розвідкам**, оскільки глобальне розгортання LoRa-мереж (IoT, smart cities) створює тисячі потенційних приймачів, а висновки роботи вже впливають на оновлення стандартів екранування кабелів у НД ТЗІ та рекомендаціях CISA щодо захисту air-gapped систем.

Автори пропонують контрзаходи, такі як випадкове шумування пікселів або екрановані кабелі з феритовими фільтрами, що знижують ефективність атаки на 90%, і робота доступна на GitHub під MIT-ліцензією для академічного використання, слугуючи основою для посилення активного зашумлення в комплексах ТЗІ.

Аналіз акустичного витоку від звичайних комп'ютерних мишей [8]

Дослідженням авторів Mauro Conti, Marin Duroyon, Gabriele Orazi та Gene Tsudik "Acoustic Side-Channel Attacks on a Computer Mouse", опублікованим на arXiv 5 травня 2025 року, було вперше системно **проаналізовано акустичні витоки від звичайних комп'ютерних мишей як потенційний канал для відновлення рухів користувача з точністю до 94% у реалістичних умовах**, розширюючи відомі атаки на HID-пристрої за межі клавіатур.

Автори детально розглянули фізичні джерела звуку: тертя коліщатка, клацання кнопок, ковзання по поверхні та вібрації оптичного сенсора, які генерують унікальні акустичні сигнатури в діапазоні 0,4–12 кГц, дозволяючи класифікувати 12 типів рухів

Акустичні витоки від звичайних комп'ютерних мишей



(наприклад, ліво/право, вгору/вниз, діагоналі, кліки) за допомогою смартфона на відстані до 3 м. Експерименти з шістьма учасниками та ML-моделями (CNN та градієнтний бустинг) показали **97% точність** для чотирьох базових рухів **у контрольованому середовищі** та **94% для 12 рухів у загальному**, з додатковим сценарієм **виявлення закриття повноекранного вікна з 91% точністю**, що демонструє витік конфіденційної інформації (наприклад, навігація в інтерфейсі). Робота еволюціонує від proof-of-concept до загальної моделі, тренованої на різноманітних даних, з акцентом на реалістичні атаки через компрометовані мікрофони (наприклад, в IoT-пристроях).

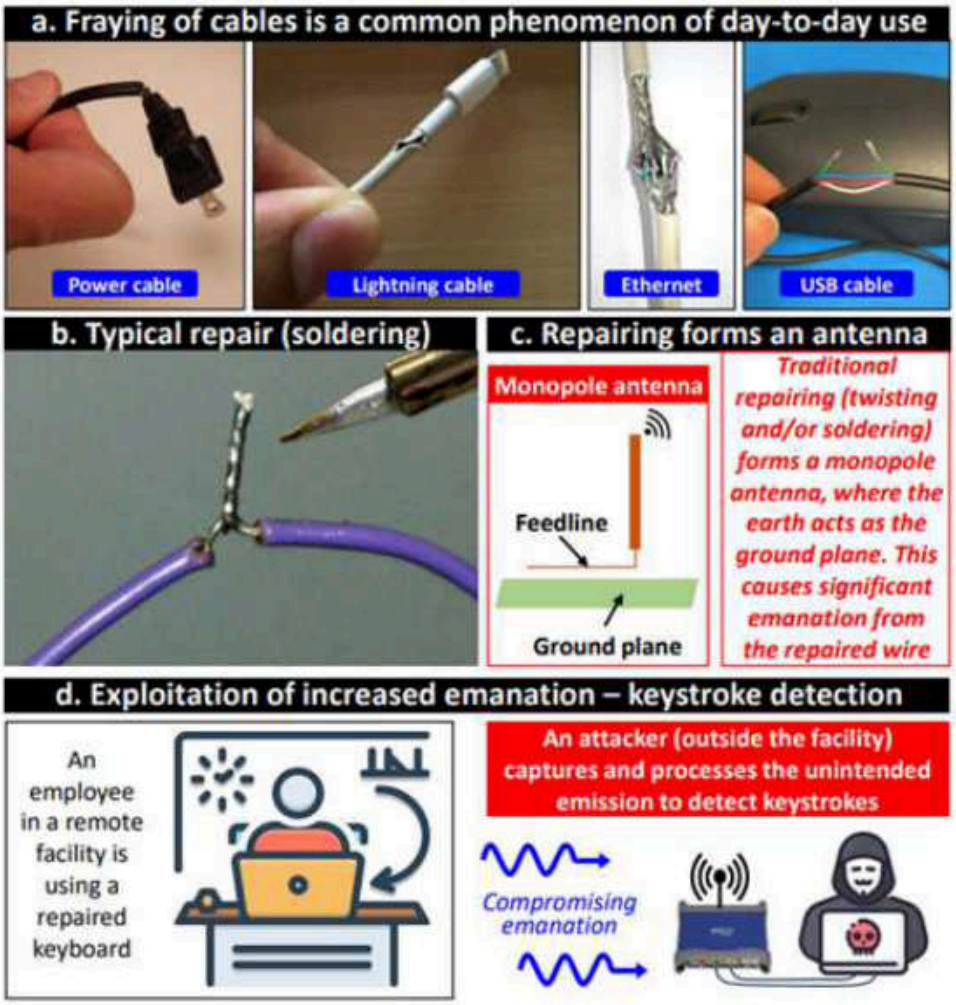
На сьогодні, у березні 2026 року, це дослідження є ключовим у тренді акустичних side-channel атак на периферію, оскільки миші залишаються основним HID у десктопах, а висновки впливають на оновлення стандартів TSI щодо активного зашумлення (наприклад, віброакустичні генератори) та паспортизації комплексів захисту. Документ оприлюднений у відкритому доступі на arXiv та ResearchGate, пропонуючи контрзаходи як-от шумові накладки на миші чи ML-детекцію аномалій, і слугує базою для захисту від комбінованих акустично-електромагнітних каналів витоку в об'єктах з обмеженим доступом.

Аналіз нової вразливості у відремонтованих USB-кабелях клавіатур [9]

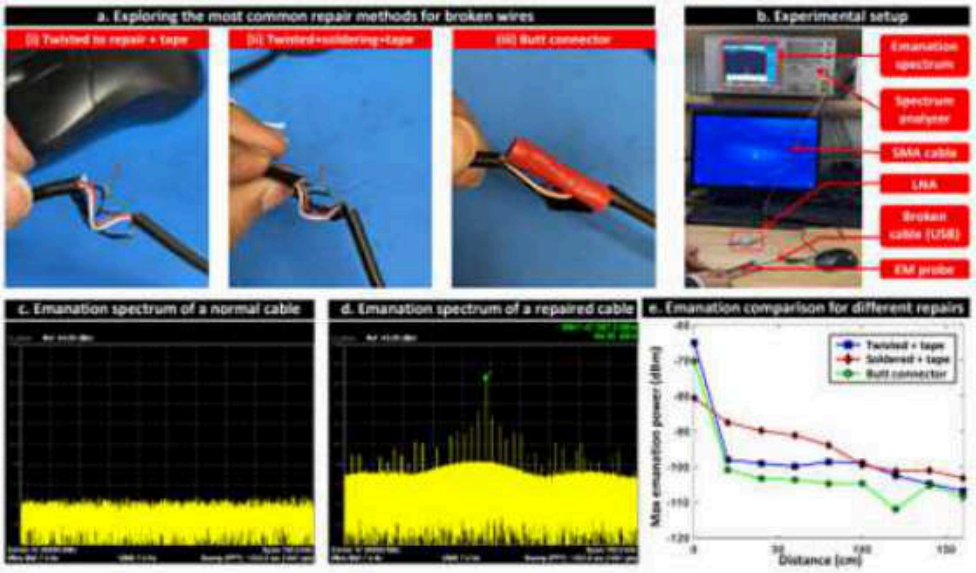
Одним із малодосліджених джерел компрометуючих електромагнітних випромінювань є зміни конструкції периферійних пристроїв, що виникають після їхнього ремонту або відновлення. Такі зміни можуть суттєво впливати на електромагнітні характеристики обладнання та формувати нові

канали витоку інформації, які відсутні у штатній конфігурації виробу. Саме дослідженню впливу ремонтних втручань на рівень побічних випромінювань і присвячена робота, результати якої наведено нижче.

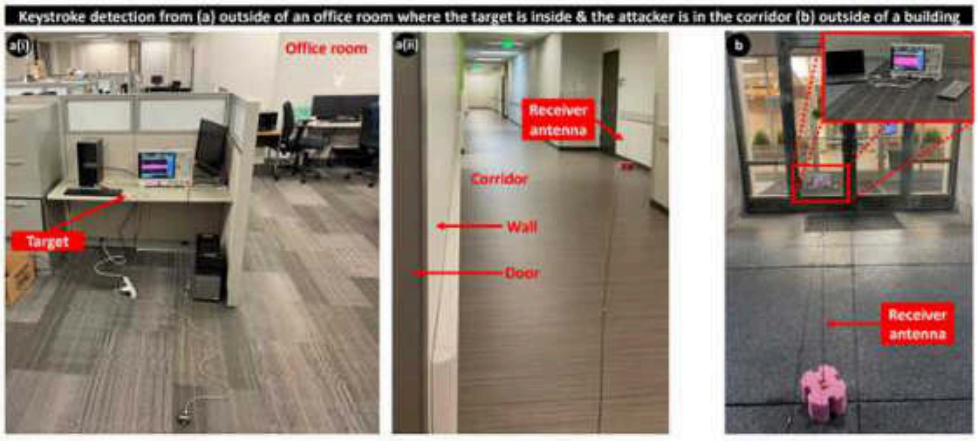
Візуалізація складової дослідження



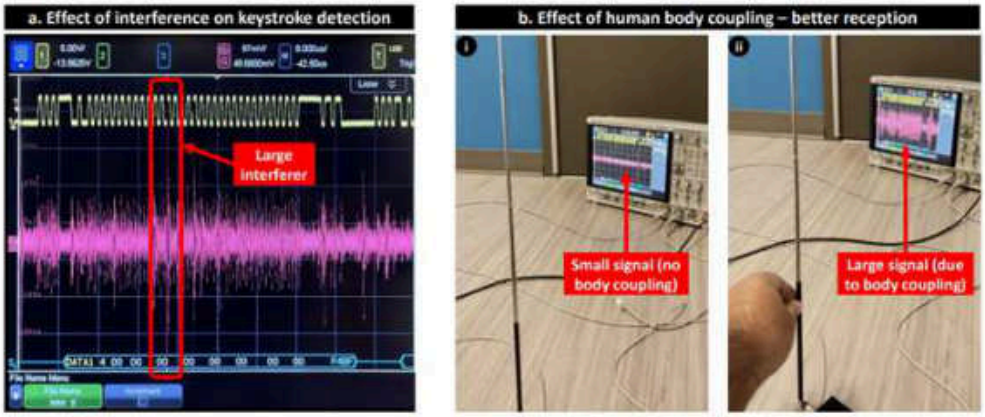
Візуалізація складової дослідження



Візуалізація складової дослідження



Візуалізація складової дослідження



> Нова вразливість

Дослідженням авторів Md Fahim Bari та колег "Keystroke Detection by Exploiting Unintended RF Emission from Repaired USB Keyboard Cables", опублікованим на arXiv у 2025 році, було розкрито нову вразливість у відремонтованих USB-кабелях клавіатур, де процес ремонту створює мініатюрну монопольну антену, посилюючи RF-випромінювання для виявлення натискань клавіш на відстані до 12 м з 100% точністю.

Автори детально проаналізували фізичні механізми: наведення від сигналів даних (5 В, 480 Мбіт/с) у пошкодженому кабелі генерують компрометуючі ЕМ-випромінювання в діапазоні 100–500 МГц, які проникають через стіни товщиною 14 см, дозволяючи відновлювати 70 різних клавіш за допомогою SDR-приймача (наприклад, USRP) у трьох середовищах (відкритий простір, коридор, зовнішня будівля).

Експерименти з трьома типами кабелів та ефективним алгоритмом детекції (на основі піків сигналу та ML-класифікації) продемонстрували стійкість до інтерференцій і ефекту тіла людини, з BER менше 0,01 на 12 м. Робота розширює класичні TEMPEST-атаки на модифіковане обладнання, показуючи, як "ремонт" посилює витік порівняно з

оригінальними кабелями (детекція лише до 4 м). На сьогодні, у березні 2026 року, це дослідження є актуальним трендом у сфері технічного захисту інформації, оскільки ремонт кабелів поширений у державних та комерційних системах, а висновки впливають на стандарти екранування (наприклад, багатошарове металеве покриття під час ремонту) та атестацію комплексів ТЗІ. Автори пропонують контрзаходи, такі як феритові фільтри та екрановані роз'єми, що знижують дальність на 90%, і робота доступна на arXiv, слугуючи основою для оновлення норм ПЕМВН щодо USB-периферії в захищених об'єктах.

Таким чином, дослідження доводить, що порушення цілісності конструкції USB-кабелю та його подальший ремонт можуть перетворювати штатні елементи периферійного обладнання на джерело інформативних побічних електромагнітних випромінювань, придатних для відновлення введених користувачем даних. Отримані результати підтверджують, що рівень захищеності інформаційної системи визначається не лише характеристиками електронних пристроїв, а й фактичним технічним станом їхніх з'єднувальних компонентів. Робота розширює сучасні уявлення про природу TEMPEST-загроз, демонструючи необхідність контролю конструктивних змін периферійного обладнання та врахування їхнього впливу під час оцінювання захищеності об'єктів інформаційної діяльності.

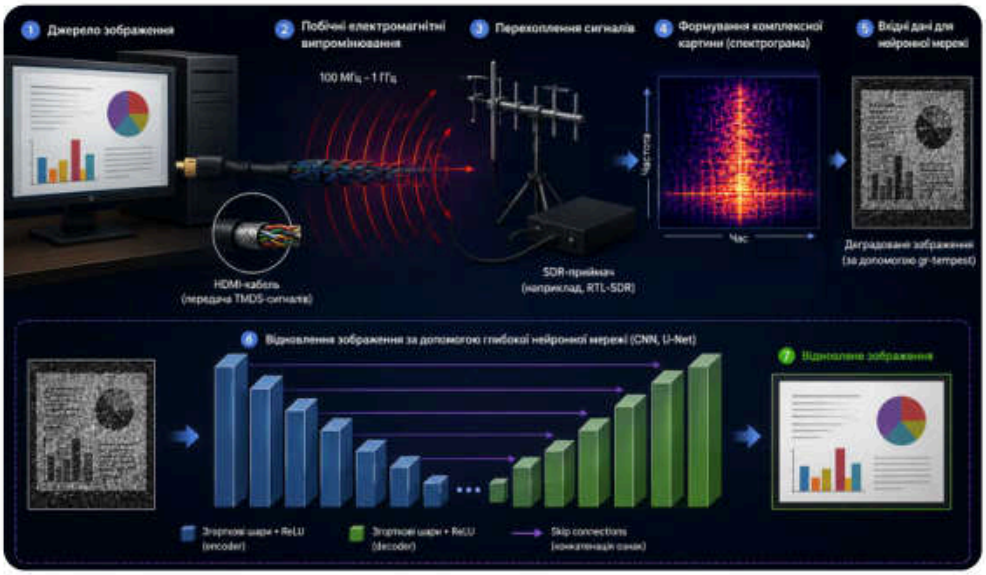
Тренд 2025–2026: Deep-TEMPEST (застосування машинного навчання для відновлення зображень за побічними електромагнітними випромінюваннями інтерфейсу HDMI) та посилення активного зашумлення периферійних пристроїв

Одним із найбільш перспективних напрямів розвитку сучасних атак побічними каналами є інтеграція технологій машинного навчання з методами аналізу компрометуючих електромагнітних випромінювань. Такий підхід дозволяє автоматизувати оброблення складних сигналів та отримувати корисну інформацію з даних, які раніше вважалися малопридатними для практичного використання.

Трендом 2025–2026 років у сфері технічного захисту інформації є розвиток Deep-TEMPEST – методів на основі глибокого навчання для відновлення зображень за побічними електромагнітними випромінюваннями інтерфейсу HDMI. У дослідженні Santiago Fernández та співавторів «Deep-TEMPEST: Using Deep Learning to Eavesdrop on HDMI from its Unintended Electromagnetic Emanations» продемонстровано можливість

реконструкції візуальної інформації шляхом аналізу електромагнітних сигналів, що виникають під час передавання даних інтерфейсом HDMI.

Авторами встановлено, що побічні електромагнітні випромінювання в діапазоні приблизно **100 МГц – 1 ГГц** можуть бути **перехоплені за допомогою SDR-приймачів** та використані для формування спотвореного зображення екрана. Для його покращення застосовано **згорткові нейронні мережі** на основі архітектури U-Net, які виконують автоматичне усунення спотворень та підвищують якість реконструкції. Експериментальні результати підтвердили можливість відновлення текстового вмісту вебоглядачів, документів та інших графічних об'єктів на відстані кількох метрів від джерела випромінювання.



Паралельно з розвитком Deep-TEMPEST удосконалюються **засоби протидії витоку інформації,** зокрема **системи активного зашумлення периферійних пристроїв**. Такі рішення формують додаткові електромагнітні або механічні завади, що ускладнюють виділення інформативних ознак із побічних випромінювань технічних засобів обробки інформації.

> Актуальна загроза

ØСтаном на 2026 рік технології Deep-TEMPEST розглядаються як один із найбільш перспективних напрямів розвитку атак побічними електромагнітними каналами, насамперед щодо ізольованих (air-gapped) інформаційних систем. Результати досліджень уже впливають на вдосконалення вимог до екранування високошвидкісних цифрових інтерфейсів та розвиток нових методів протидії витоку інформації через ПЕМВН.

Таким чином, дослідження Deep-TEMPEST підтверджує, що **сучасні алгоритми глибокого навчання** суттєво розширюють можливості **аналізу побічних електромагнітних випромінювань** і **підвищують ефективність відновлення інформації з технічних каналів витоку**. Це зумовлює необхідність подальшого розвитку комплексних засобів захисту, здатних протидіяти атакам нового покоління, що поєднують методи TEMPEST та машинного навчання.

Перелік джерел посилання

1. Rzemieniuk M., Niewiarowski A., Książek W. Acoustic Side-Channel Vulnerabilities in Keyboard Input Explored Through Convolutional Neural Network Modeling: A Pilot Study. Applied Sciences. Basel : MDPI, 2026. Vol. 16, No. 2. Article 563. 23 p. DOI: 10.3390/app16020563
2. Wang J., Wang X., Luo Z., Ouyang Q., Zhou C., Wang H. Recent Advances in Deep-Learning Side-Channel Attacks on AES Implementations. Computers, Materials & Continua. Henderson : Tech Science Press, 2026. Vol. 87, No. 1. Article 3. DOI: 10.32604/cmc.2025.074473
3. Cheng Y., Zhu S., Ou C., Han X., Li Y., Zheng S. Capacitive Touchscreens at Risk: Recovering Handwritten Trajectory on Smartphone via Electromagnetic Emanations. arXiv preprint. Ithaca, NY : arXiv, 2025. arxiv.org/abs/2512.11484
4. Yang K., Zhang Y., Li T., Sun L. ASIDS: Acoustic Side-Channel Based Intrusion Detection System for Industrial Robotic Arms. Computers & Security. Amsterdam : Elsevier Ltd., 2025. Vol. 157. Article 104586. DOI: 10.1016/j.cose.2025.104586
5. Ковбасюк О., Башкиров О., Ковалько О., Ступак С. Сучасні матеріали і технології покращення екранування побічних електромагнітних випромінювань та наведень електронної техніки. Озброєння та військова техніка. Київ : ЦНДІ ОВТ ЗС України, 2025. Т. 48, № 4. С. 60–68. DOI: 10.34169/2414-0651.2025.4(48).60-68
6. Ghazi Asgar S. A., Reddy N. QuietPrint: Protecting 3D Printers Against Acoustic Side-Channel Attacks. Proceedings of the 12th ACM Cyber-Physical System Security Workshop (CPSS '26). New York, NY : ACM, 2026. P. 25–34. DOI: 10.1145/3775042.3807880
7. Sun X., Zheng Y., Xi W., Chen Z., Chen Z., Hao H., Jiang Z., Zhong S. TEMPEST-LoRa: Cross-Technology Covert Communication. Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), October 13–17, 2025, Taipei, Taiwan. New York, NY : ACM, 2025. 17 p. DOI: 10.1145/3719027.3744817
8. Conti M., Duroyon M., Orazi G., Tsudik G. Acoustic Side-Channel Attacks on a Computer Mouse. Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2024. Lecture Notes in Computer Science. Cham : Springer, 2024. Vol. 14828. P. 44–63. DOI: 10.1007/978-3-031-64171-8_3
9. Bari M. F., Xie Y., Choudhury M. R., Sen S. Keystroke Detection by Exploiting Unintended RF Emission from Repaired USB Keyboards. arXiv preprint. Ithaca, NY : arXiv, 2025. DOI: 10.48550/arXiv.2509.00043
10. Fernández S., Martínez E., Varela G., Musé P., Larroca F. Deep-TEMPEST: Using Deep Learning to Eavesdrop on HDMI from its Unintended Electromagnetic Emanations. Proceedings of Submitted. New York, NY : ACM, 2024. 10 p. DOI: 10.48550/arXiv.2407.09717

КОНТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ:

системи технічного захисту інформації

Інформаційний бюлетень
№2 ◦ 2026

Заснований у 2026 році
Виходить щомісяця

Відповідальний за дизайн та верстку:
Ольга ІНКАРБАЄВА, ДержНДІ технологій кібербезпеки.

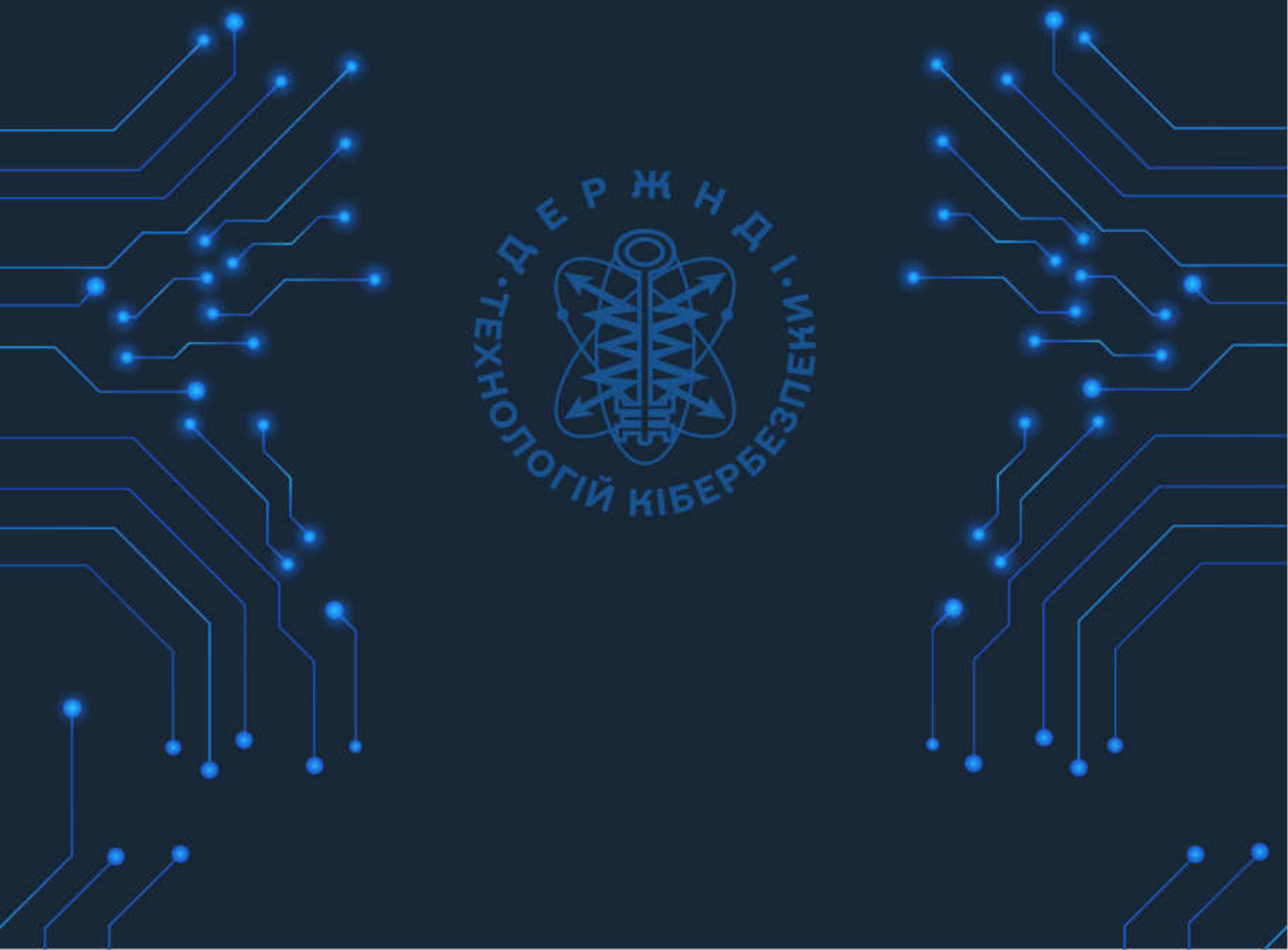
Наклад 50 примірників

Засновник:
Адміністрація Державної служби спеціального зв'язку
та захисту інформації України, 2026 рік

Видавець:
Державний науково-дослідний інститут
технологій кібербезпеки та захисту інформації
03142, вул. М. Залізняка 3, корп. 6, м. Київ, Україна
Тел.: 38 (044) 281-85-20, (044) 281-97-11, e-mail: ictip@cip.gov.ua
веб-сайт: csi.cip.gov.ua, Facebook: www.facebook.com/cybersec.sci,
Instagram: www.instagram.com/cybersec.sci

Свідоцтво суб'єкта видавничої справи ДК №8727 від 19 серпня 2026 року
Ідентифікатор медіа R30-07316
Рішення Національної ради України з питань телебачення і радіомовлення
№1652 від 25 червня 2026 року

Матеріали інформаційного бюлетеня можуть бути використані
з посиланням на джерело.


ДЕРЖНДІ ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ