УДК 004.056.53

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ НА РОБОЧОМУ МІСЦІ ВІД ПЕРЕХОПЛЕННЯ ПЕМВ ШЛЯХОМ ПРИМУСОВОЇ АКТИВАЦІЇ HDCP

Ярмола А.В., Ликов Ю.В., Ликова Г.О.
e-mail: yurii.lykov@nure.ua
Харківський національний університет радіоелектроніки, каф. ІРТЗІ,
м. Харків, Україна

This paper addresses the risk of information leakage from computer displays through compromising electromagnetic emanations (TEMPEST/Van Eck). We propose a practical “HDCP-for-Privacy” concept: instead of enabling HDCP only for DRM-protected video, the display link (HDMI/DisplayPort) is forced to stay encrypted during everyday office work (documents, web applications, e-mail). We outline a passive interception model focused on interface cables and compare common video interfaces by reconstruction complexity. The implementation approach relies on OS-level control (Linux DRM/KMS content-protection properties and Windows output-protection mechanisms) plus a low-cost USB indicator that provides immediate visual assurance of the HDCP state. Link encryption reduces correlation between emitted signals and pixel content at the cable level, raising the bar for practical TEMPEST attacks.

Проблематика технічних каналів витоку інформації через побічні електромагнітні випромінювання (ПЕМВ) залишається актуальною для робочих місць, де обробляються персональні дані та службова інформація. TEMPEST-сценарій передбачає пасивне спостереження: противник не підключається до ПК та не втручається в ОС, але приймає випромінювання, що корелює з відеосигналом. За наявності достатнього відношення сигнал/шум можлива синхронізація з розгорткою та реконструкція зображення, включно з читабельним текстом, що робить відеотракт одним із найбільш інформативних технічних каналів витоку.

Джерелами ПЕМВ у відеотракті виступають високошвидкісні драйвери фізичного рівня (PHY), кабель і роз’єми, перехідники, док-станції та елементи заземлення. Особливо критичним є інтерфейсний кабель, який може працювати як антена. Навіть у цифрових інтерфейсах випромінювання містить регулярні спектральні компоненти, пов’язані з піксельним тактом, лінійним кодуванням або пакетною структурою, що спрощує пошук частот і відновлення синхронізації у приймачі SDR.

З точки зору стійкості до ПЕМВ-перехоплення інтерфейс VGA є найгіршим варіантом: аналогові рівні RGB безпосередньо відображають яскравість/колір пікселів, а HSYNC/VSYNC забезпечують часові маркери. Цифрові інтерфейси DVI/HDMI (TMDS) та DisplayPort використовують диференційну передачу і кодування, тому відновлення пікселів із ПЕМВ є складнішим і зазвичай вимагає відновлення тактування та декодування по-

току. Внутрішні інтерфейси LVDS/eDP мають малий розмах сигналу і короткі траси, що зменшує дальність перехоплення, однак у межах корпусу дисплея можуть залишатися локальні витоки.

Ключовою ідеєю роботи є застосування High-bandwidth Digital Content Protection (HDCP) як додаткового бар'єра проти реконструкції інформації з ПЕМВ. Традиційно HDCP використовується для захисту авторського контенту та активується епізодично. Натомість пропонується концепція HDCP-for-Privacy: примусово підтримувати шифрування лінка "GPU—монітор" під час звичайної роботи з документами, веб-ресурсами та прикладними системами. У такому режимі сигнал на кабелі (HDMI/DP) є шифртекстом, і навіть при якісному радіоприйомі противник отримує некорельований із зображенням потік, що підвищує поріг атаки.

Практична реалізація HDCP-for-Privacy вимагає не лише одноразового ввімкнення, а забезпечення стабільного стану Enabled упродовж сеансу. Події sleep/resume, hot-plug, зміна частоти, підключення док-станції або MST-хаба можуть викликати повторну аутентифікацію чи деградацію (Undesired/Disabled). Тому політика має включати: (1) автоматичне встановлення бажаного стану захисту, (2) перевірку фактичного стану, (3) журналювання причин відмови, (4) контроль допустимого складу тракту (сертифіковані кабелі, заборона HDMI→VGA конвертерів тощо).

Для Linux точкою керування є DRM/KMS, де для багатьох драйверів доступна властивість конектора "Content Protection" із переходом у "Desired" та "Enabled". Це дає змогу реалізувати агент або systemd-службу, що реагує на udev-події дисплея і повторює ініціацію HDCP, фіксуючи тайм-аути та несумісність приймача. У Windows відсутній універсальний глобальний перемикач "завжди HDCP", однак існують механізми захисту виходу (output protection), які можна використати в агенті політик: застосунок/служба запитує захищений вивід, перевіряє статус на активних моніторах, відслідковує зміни топології і формує події для адміністратора. Для SoC+Android можливість примусу залежить від вендорської реалізації HDMI/DP-контролера і DRM-пайплайна (secure surfaces), тому найбільш реалістичним є підхід із контрольованими прошивками/конфігураціями та моніторингом стану через системні логи.

Окремою задачею є операційна перевірюваність: у стандартних інтерфейсах ОС факт активного HDCP часто невидимий для користувача. Щоб уникнути помилкової впевненості, пропонується USB-індикатор стану HDCP, який отримує команду від агента ОС (HID/CDC) і відображає агрегований стан: зелений—усі активні зовнішні виходи у Enabled; жовтий—перевірка/переаутентифікація; червоний—відмова або невизначеність. Fail-safe поведінка (перехід у червоний при втраті heartbeat) підвищує надійність контролю.

Для практичного впровадження доцільно використовувати короткий чек-лист: (а) переходити на HDMI/DP і виключати VGA та аналогові кон-

вертери; (б) застосовувати якісні екрановані кабелі мінімальної довжини, зменшуючи кількість перехідників; (в) стандартизувати монітори/док-станції за ознакою коректної HDCP-аутентифікації; (г) запускати агент політики, що повторює ініціацію HDCP після hot-plug/sleep і веде журнал станів; (д) забезпечити візуальну індикацію (USB-LED) та регламент реагування у разі переходу в Undesired/Disabled.

Критичним аспектом є контроль сумісності: сплітери, KVM-перемикачі та активні перехідники можуть змінювати топологію тракту і зривати аутентифікацію, а отже — вимикати шифрування. У корпоративному середовищі доцільно вести перелік дозволених моделей, тестувати типові режими (роздільність/частота/HDR) та фіксувати метрики стабільності (частка часу в Enabled, середній час переаутентифікації, причини відмов). Це перетворює HDCP-for-Privacy з одноразового налаштування на керований процес технічного захисту інформації з елементами аудиту та безперервного вдосконалення.

У підсумку, HDCP-for-Privacy є технологічно доступним компенсуючим контролем “середнього рівня” між відсутністю захисту та дорогими TEMPEST-рішеннями. Підхід не усуває випромінювання як фізичне явище і не перекриває витоки поза лінком (внутрішні вузли дисплея, живлення, програмні канали), однак суттєво ускладнює пасивне перехоплення саме з кабельного тракту та підвищує керованість режиму захисту за рахунок автоматизації й індикації.

Список використаних джерел:

1. Van Eck W. Electromagnetic radiation from video display units: An eavesdropping risk? // Computers & Security. 1985. Vol. 4, № 4. P. 269–286.

2. Kuhn M. G., Anderson R. J. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations // Information Hiding (IH’98). LNCS 1525. Springer, 1998. P. 124–142.

3. Digital Content Protection LLC. High-bandwidth Digital Content Protection System, Revision 1.4. 2009.

4. Microsoft. Output Protection Manager (OPM) (Media Foundation) : документація. URL: https://learn.microsoft.com/windows/win32/medfound/output-protection-manager (дата звернення: 17.03.2026).

5. The Linux Kernel documentation. DRM/KMS: Content Protection (HDCP) properties. URL: https://docs.kernel.org/gpu/drm-kms.html (дата звернення: 17.03.2026).