УДК 621.397.43:004.056

Ільчук Артем
Галина Крайнічук (Шелепало)

ВРАЗЛИВОСТІ IP-КАМЕР ЯК ВЕКТОР КІБЕРЗАГРОЗ: АНАЛІЗ ТА МЕТОДИ ЗАХИСТУ

Вінницький національний технічний університет, м. Вінниця

Анотація *У роботі проведено аналіз актуальних загроз інформаційній безпеці, пов'язаних із вразливостями IP-камер у системах відеонагляду. Розглянуто статистику незахищених пристроїв за даними пошукової системи Shodan, класифіковано відомі CVE-вразливості та типові вектори атак на IP-камери. Проаналізовано наслідки компрометації систем відеоспостереження: від витоку відеоданих до використання камер як плацдарму для атак на внутрішню мережу. Запропоновано комплекс технічних та організаційних заходів захисту, зокрема застосування VPN-тунелювання на основі WireGuard як методу ізоляції відеотрафіку від відкритої мережі.*

Ключові слова: IP-камери, відеонагляд, кібербезпека, вразливості, CVE, Shodan, VPN, WireGuard, RTSP, захист мережі.

Abstract *This paper analyses current cybersecurity threats related to vulnerabilities in IP cameras used in video surveillance systems. Statistics on exposed devices from the Shodan search engine are reviewed, known CVE vulnerabilities are classified, and typical attack vectors against IP cameras are examined. The consequences of video surveillance system compromise are discussed, ranging from video data leakage to using cameras as a foothold for attacks on internal networks. A set of technical and organisational security measures is proposed, including VPN tunnelling based on WireGuard as a method for isolating video traffic from public networks.*

Keywords: IP cameras, video surveillance, cybersecurity, vulnerabilities, CVE, Shodan, VPN, WireGuard, RTSP, network security.

Вступ

Системи відеонагляду на основі IP-камер набули масового поширення у житловому секторі, на об'єктах критичної інфраструктури та промислових підприємствах. Разом із тим, за даними дослідницької компанії Bitdefender, понад 34 % підключених до Інтернету IP-камер мають критичні або високі вразливості у програмному забезпеченні [1]. Пошукова система Shodan індексує мільйони відкритих відеопристроїв по всьому світу, значна частина яких доступна без будь-якої автентифікації [6]. Така ситуація перетворює IP-камери з інструменту безпеки на вектор кіберзагроз, що вимагає системного аналізу та розробки методів захисту.

Аналіз вразливостей IP-камер та масштаб проблеми

Дослідження у сфері безпеки IP-пристроїв відеонагляду виявили кілька системних класів вразливостей [4, 5]. По-перше, переважна більшість виробників постачають камери із заводськими обліковими даними (admin/admin, admin/12345), які користувачі рідко змінюють. За даними роботи [6], понад 60 % скомпрометованих IP-камер були зламані саме через незмінені заводські паролі. По-друге, прошивки IP-камер часто містять відомі CVE-вразливості, які залишаються невиправленими роками: виробник припиняє підтримку пристрою задовго до закінчення строку його фактичної експлуатації.

Протокол RTSP (Real Time Streaming Protocol), що використовується переважною більшістю IP-камер для передачі відеопотоку, за замовчуванням не передбачає шифрування. Це означає, що перехоплення відеопотоку у незахищеній мережі є тривіальним завданням для зловмисника. Costin [4] класифікував атаки на системи відеонагляду за чотирма векторами: мережеві атаки (перехоплення RTSP, MITM), атаки на вебінтерфейс (XSS, CSRF, обхід автентифікації), атаки на прошивку (переповнення буфера, впровадження команд) та атаки через хмарну інфраструктуру виробника.

За даними пошукової системи Shodan значну частку підключених до Інтернету пристроїв становлять IP-камери з відкритими портами 554 (RTSP), 80/8080 (HTTP вебінтерфейс) та 37777 (Dahua) [6]. Аналіз результатів пошуку за запитом «RTSP camera» виявляє тисячі камер, відеопотік з яких доступний без автентифікації в реальному часі. Масштабним інцидентом є ботнет Mirai, який скомпрометував понад 600 000 IoT-пристроїв, серед яких IP-камери становили найбільшу частку, і здійснив наймасштабнішу DDoS-атаку в історії з пропускною здатністю понад 1 Тбіт/с [5].

Дослідження Kalbo et al. [6] показує, що атаки на IP-системи відеонагляду реалізуються на трьох рівнях: фізичному (несанкціонований доступ до пристрою), мережевому (перехоплення незашифрованого RTSP-потоку, ARP-спуфінг) та програмному (вразливості прошивки, хмарного API).

Особливу небезпеку становить останній вектор: компрометація хмарного сервісу виробника надає зловмиснику доступ одразу до всіх підключених до нього пристроїв.

Методи захисту відеотрафіку та порівняльний аналіз

Аналіз існуючих підходів до захисту IP-систем відеонагляду [1-5] дозволяє виділити три основні стратегії. Перша – сегментація мережі: розміщення камер в ізольованій VLAN із забороною прямого доступу з Інтернету. Ефективна, але потребує керованої мережевої інфраструктури та недоступна для мобільних або розподілених інсталяцій. Друга – RTSP over TLS: шифрування відеопотоку на транспортному рівні. Підтримується лише частиною пристроїв. Третя – VPN-тунелювання: інкапсуляція всього відеотрафіку у зашифрований тунель між камерою та сервером.

VPN-тунелювання на основі протоколу WireGuard є найбільш універсальним підходом, оскільки не залежить від підтримки шифрування конкретним пристроєм [7]. Відеопотік шифрується алгоритмом ChaCha20-Poly1305 (256-бітний ключ) до виходу у будь-який канал зв'язку – відкрита мережа, Wi-Fi або 4G – і розшифровується лише на авторизованому сервері. Аутентифікація на основі криптографічного ключа Curve25519 унеможливлює підключення без знання приватного ключа (обчислювальна складність близько 2^{128} операцій). Принципово, що медіасервер прив'язується до внутрішнього VPN-інтерфейсу і стає фізично невидимим з відкритої мережі. У табл. 1 наведено порівняння підходів до захисту RTSP-відеопотоку за ключовими критеріями безпеки.

Таблиця 1 – Порівняння методів захисту RTSP-відеопотоку

Критерій	**Без захисту**	**VLAN сегментація**	**RTSP over TLS**	**VPN (WireGuard)**	**Хмара виробника**
Шифрування трафіку	Ні	Ні	TLS 1.2+	ChaCha20 256 біт	AES-128 (сервер)
Видимість у мережі	Відкрита	Ізольована	Відкрита	Прихована (VPN)	Хмара вир.
Аутентифікація	Пароль	Пароль	Сертифікат TLS	Curve25519 ключ	Акаунт вир.
Захист від Mirai/brute-force	Ні	Частково	Частково	Так	Частково
Залежність від виробника	Низька	Низька	Низька	Відсутня	Критична
Мобільна інсталяція (4G)	Так	Ні	Так	Так	Так

Висновки

Проведений аналіз показав, що IP-камери є одним із найвразливіших класів підключених пристроїв: стандартні паролі, невиправлені CVE-вразливості та передача відеопотоку у відкритому вигляді через RTSP перетворюють системи відеонагляду на вектор масштабних кібератак, що підтверджується інцидентом ботнету Mirai. Найбільш ефективним підходом з точки зору рівня захисту, незалежності від виробника та сумісності з мобільними мережами є VPN-тунелювання з використанням WireGuard: наскрізне шифрування ChaCha20-Poly1305, аутентифікація Curve25519 та повна ізоляція медіасервісів від відкритої мережі незалежно від типу каналу зв'язку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Chamasemani F. F., Affendey L. S. Systematic review and classification on video surveillance systems. International Journal of Information Technology and Computer Science. 2013. Vol. 5, No. 7. P. 87-96.
URL: https://www.mecs-press.org/ijitcs/ijitcs-v5-n7/v5n7-11.html. (Дата звернення 02.06.2026)
2. Tsakanikas V., Dagiuklas T. Video surveillance systems – current status and future trends. Computers & Electrical Engineering. 2018. Vol. 70. P. 736-753. URL: https://doi.org/10.1016/j.compeleceng.2017.11.011
3. Golovin O. M., Sapunova N. O. Evoliutsiia system videospostezhennia. Information Technologies and Systems. 2025. Vol. 3, No. 3. P. 56-75. URL: https://nasu-periodicals.org.ua/index.php/its/article/view/20080/20943 (Дата звернення 02.06.2026)
4. Costin A. Security of CCTV and video surveillance systems: threats, vulnerabilities, attacks, and mitigations. Proc. 6th Intl. Workshop on Trustworthy Embedded Devices. Vienna, 2016. P. 45-54. URL: https://www.researchgate.net/publication/307866768
5. Vennam P. et al. Attacks and preventive measures on video surveillance systems: a review. Applied Sciences. 2021. Vol. 11, No. 12. P. 5571. URL: https://doi.org/10.3390/app11125571
6. Kalbo N., Mirsky Y., Shabtai A., Elovici Y. The security of IP-based video surveillance systems. Sensors. 2020. Vol. 20, No. 17. P. 4806. URL: https://arxiv.org/abs/1910.10749 (Дата звернення 02.06.2026)
7. Raja A. IoT Security by Design. IoT For All. URL: https://www.iotforall.com/iot-security-by-design (Дата звернення 02.06.2026)

Ільчук Артем Олександрович – студент групи БКС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця. E-mail: ilchuk1414@gmail.com

Шелепало (Крайнічук) Галина Василівна – к.фіз-мат.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця. E-mail: hv.shelepalo@vntu.edu.ua

Ilchuk Artem Oleksandrovych – student of the group BKS-22b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Shelepalo (Krainichuk) Halyna Vasylivna – Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Information Security, Vinnytsia National Technical University, Vinnytsia.