

АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДОМАШНІХ ПРИСТРОЇВ ІОТ НА ПРИКЛАДІ КАМЕРИ ВІДЕОНАГЛЯДУ TP-LINK TAPО

Головашич Даниїл

Здобувач вищої освіти

Львівський державний університет безпеки життєдіяльності

Полотай Орест

к.т.н., доцент, науковий керівник

Львівський державний університет безпеки життєдіяльності

Сьогодні все більша кількість людей користуються пристроями розумного будинку: камери відеоспостереження, датчики, системи освітлення, роботи пилососи та інше обладнання, яким можна керувати через мережу Інтернет. Але такі пристрої не завжди добре захищені від несанкціонованого доступу, особливо якщо це пристрої сумнівних виробників. Особливо це стосується IP-камер, адже вони записують відео, передають його через мережу та дають змогу керувати своїми функціями за допомогою мобільного застосунку. Якщо в такому пристрої є вразливості, сторонні особи можуть спробувати отримати несанкціонований доступ до потокового відео, локального сховища пристрою або налаштувань камери.

Питання інформаційної та кібербезпеки набуває щораз більшої актуальності та важливості, тому що комп'ютери, смартфони та інші цифрові пристрої використовуються майже всюди і цілодобово. Також підвищується професійна майстерність зловмисників і кількість способів викрадення даних та проникнення до приватних мереж. Захищати потрібно не тільки важливу державну чи службову інформацію, але й особисті дані, фінансову інформацію та відомості про приватне життя людей. Окрему небезпеку становлять спроби сторонніх осіб отримати несанкціонований доступ до приватного житла за допомогою сучасних технічних засобів. Крім того, онлайн камери спостереження, можуть використовуватися і в державних установах та об'єктах критичної інфраструктури, системах відеонагляду міста.

Звідси випливає необхідність забезпечення безпеки даних, які обробляються такими системами відеоспостереження. Серед сучасних доступних варіантів онлайн спостереження є пристрої серії TP-Link Tapo , які дають змогу відслідковувати певну територію та керувати камерою через мобільний застосунок. Проте під час їх використання потрібно враховувати не лише зручність, а й можливі загрози для інформаційної безпеки [2]. На рисунку 1 зображено камеру відеоспостереження TP-Link Tapo C200.



Рисунок 1 – Розумна камера відеоспостереження TP-Link Tapo C200 [5]

Домашня IP-камера TP-Link Tapo C200 є частиною інформаційної інфраструктури. Її безпека залежить не лише від технічних характеристик самого пристрою, а й від захищеності бездротової мережі, облікового запису користувача, мобільного застосунку та вбудованого програмного забезпечення (прошивки) камери. Несанкціонований доступ до будь-якого з цих компонентів може вплинути на конфіденційність відеоданих або доступність системи відеонагляду, тобто порушити основні властивості інформації.

На даний час, розумні IoT-пристрої все частіше використовуються в побуті. Однак чим більше таких пристроїв підключено до домашньої мережі, тим більше виникає можливих проблем із безпекою. Особливо це стосується IP-камер, які записують відео, передають його через мережу Інтернет та дають змогу переглядати потокове відео і керувати налаштуваннями через мобільний застосунок. Деякі моделі також використовують хмарні сервіси для зберігання та обробки даних. Якщо камера має слабкі місця в захисті, сторонні особи можуть отримати несанкціонований доступ як до відео в режимі реального часу так і відеозаписів, змінити налаштування пристрою або порушити його нормальну роботу.

Якщо перерахувати всі загрози інформаційної та кібербезпеки камери TP-Link Tapo C200, то їх можна згрупувати у вигляді рисунку 2.



Рисунок 2 – Загрози інформаційної безпеки розумної камери відеоспостереження TP-Link Таро С200 [розроблено авторами]

Серед всіх загроз, які продемонстровані на рис. 2, нами було проаналізовано три основні категорії загроз. Перша стосується несанкціонованого доступу до камери внаслідок компрометації облікових даних або неналежного захисту мережевих сервісів. Друга пов'язана з експлуатацією вразливостей програмного забезпечення, що може призвести до збоїв у роботі пристрою або несанкціонованого доступу. Третя категорія охоплює порушення конфіденційності через неналежне керування доступом до відеозаписів, налаштуваннями приватності та обліковими записами користувачів.

Важливість перевірки безпеки таких пристроїв підтверджують і випадки виявлення вразливостей у камерах TP-Link. Наприклад, у квітні 2026 року компанія повідомила про проблему з камерою Таро С200 третьої апаратної версії (V3). Цій вразливості присвоїли номер CVE-2026-0919. Проблема полягала в тому, що камера могла неправильно обробляти занадто довгі інтернет-адреси (URL). Через це пристрій міг перестати нормально працювати. Така ситуація називається відмовою в обслуговуванні (DoS). Простими словами, камера могла тимчасово стати недоступною для користувача, через що він не зміг би нормально переглядати відео або користуватися іншими її функціями.

Для вирішення цієї проблеми виробник випустив оновлення програмного забезпечення камери – прошивку версії 1.2.6 Build 260328. Це оновлення призначене саме для третьої апаратної версії Таро С200. Наведений випадок показує, що навіть звичайні домашні камери можуть мати помилки в програмному забезпеченні. Якщо такі помилки не виправляти, вони можуть

порушувати роботу пристрою та заважати користувачеві стежити за власним помешканням. Саме тому важливо перевіряти наявність оновлень і вчасно встановлювати їх, щоб зменшити ризик виникнення подібних проблем [3].

Ще одним прикладом є вразливість CVE-2025-14553, яка щільно пов'язана з потенційним витокom хешів паролів через API вразливих версій мобільного застосунку Таро. Виробник зазначає, що ця проблема могла полегшити відновлення облікових даних шляхом офлайн-атак методом перебору (brute-force), що згодом дало б змогу зловмиснику отримати доступ до камери через локальну мережу [4] для адміністрування. Цей випадок підкреслює необхідність комплексного підходу до безпеки IoT-екосистеми, що охоплює взаємодію між пристроєм, застосунком і мережевим середовищем.

За своєю природою CVE-2026-0919 належить до класу вразливостей типу «відмова в обслуговуванні» (DoS). На відміну від вразливостей, які безпосередньо дають можливість зловмиснику здійснити крадіжку конфіденційних даних або змінити системні налаштування, ця проблема насамперед загрожує доступності пристрою. Успішна експлуатація вразливості може призвести до того, що камера тимчасово припинить виконання своїх основних функцій, таких як надання доступу до відеопотоку та моніторинг контрольованої зони. Виробник зазначає, що для спричинення описаного збою зловмиснику не потрібно проходити автентифікацію. Згідно з описом виробника, першопричина вразливості полягає в роботі HTTP-парсера – програмного компонента, який аналізує вхідні HTTP-запити та передає їхні складові частини для подальшої обробки. У нормальних умовах такий компонент повинен коректно обробляти запити різної довжини, перевіряти їхні параметри та безпечно завершувати обробку некоректно сформованих даних. Однак у моделі Таро C210 V3 виникає логічна помилка під час обробки некоректних адрес – зокрема, запитів, що містять надмірно довгий шлях у URL.

Ключовим аспектом проблеми є те, що після виявлення недійсного URL виконання програми переходить до процедури очищення ресурсів. Ця процедура покладається на наявність буферів пам'яті, які за певних умов могли бути виділені неналежним чином. У результаті програма намагається виконати операції з ресурсами, що перебувають у непередбаченому стані, що призводить до аварійної зупинки відповідної служби. Виробник описує таку послідовність подій: неправильна обробка надмірно довгого URL, помилка під час очищення ресурсів, аварійна зупинка служби та перезавантаження пристрою.

Основним заходом для усунення проблеми є оновлення мікропрограми камери до версії, в якій виробник виправив цю вразливість. За даними TP-Link, вразливими є версії мікропрограми, старіші за 1.2.6 Build 260328, для моделі Таро C210 (апаратна версія V3). Користувачам слід перевіряти наявність оновлень саме для апаратної версії свого пристрою, оскільки мікропрограми для різних апаратних ревізій можуть бути несумісними [1].

Також доцільно вжити таких заходів:

1. Обмеження доступу до мережі: не відкривайте доступ до сервісів камери з Інтернету без вагомих причин; перевірте правила перенаправлення портів (port forwarding) на маршрутизаторі.

2. Ізоляція IoT-пристроїв: якщо маршрутизатор підтримує таку функцію, розмістіть камери в окремій мережі або VLAN, обмеживши їхню взаємодію з комп'ютерами та іншими пристроями в домашній мережі.

3. Оновлення мікропрограми (firmware): періодично перевіряйте наявність оновлень через застосунок Таро або на офіційному вебсайті виробника.

4. Моніторинг доступності: звертайте увагу на часті перезавантаження камери, незаплановані переривання відеопотоку та іншу нетипову поведінку пристрою. Однак самі по собі такі випадки не свідчать про експлуатацію вразливості CVE-2026-0919.

Ще однією загрозою інформаційній безпеці екосистеми TP-Link Таро є вразливість CVE-2025-14553, пов'язана з розкриттям хешованих паролів через API мобільного застосунку Таро. На відміну від CVE-2026-0919, що переважно впливає на доступність камери, ця вразливість стосується захисту автентифікаційних даних і потенційно може загрожувати конфіденційності облікового запису.

Хешування паролів необхідне для того, щоб вони не зберігалися і не передавалися у звичайному вигляді. Але це не означає, що пароль повністю захищений. Якщо хеш потрапить у бік, вони можуть спробувати підібрати пароль за допомогою словників або багаторазового перебору різних варіантів. Те, наскільки успішною є така спроба, залежить від способу хешування і складності самого пароля. Тому отримання хешу ще не означає, що зловмисник одразу зможе керувати камерою, але створює додатковий ризик безпеки облікового запису.

За інформацією компанії TP-Link, проблема пов'язана з мобільним додатком Таро. Через одну з його функцій можна отримати пароль без попередньої перевірки особистості користувача. Якщо зловмисник має доступ до відповідної частини локальної мережі, він може отримати ці дані та спробувати вибрати пароль без підключення до камери. Якщо йому це вдасться, він може отримати права адміністратора і керувати вразливим пристроєм через локальну мережу. За шкалою CVSS 4.0 виробник оцінив цю проблему в 7,0 бали, що вказує на високий рівень небезпеки. Найбільші ризики полягають у можливому перегляді відео без дозволу власника та втрати контролю над камерою. У той же час для успішної атаки необхідно мати доступ до локальної мережі та відновити пароль із його хеша. Проблема стосується версій програми Таро старше 3.1.601 для iOS та 3.1.6 для Android. Щоб усунути вразливість, достатньо оновити мобільний додаток. Для цього не потрібно оновлювати програмне забезпечення самої камери.

Таким чином, випадок із вразливістю CVE-2025-14553 показує, що захист розумної камери залежить не тільки від програмного забезпечення, встановленого на пристрої. Не менш важливою є безпека мобільної програми, через яку користувач налаштовує камеру та керує її роботою. Щоб знизити ризик злому, необхідно вчасно встановлювати оновлення Таро, використовувати

складний та унікальний пароль та не допускати підключення сторонніх осіб до домашньої мережі Wi-Fi.

Аналіз загроз для домашніх пристроїв IoT на прикладі камер TP-Link Таро показує, що для їх захисту потрібно враховувати різні можливі проблеми. Серед них – перегляд відео сторонніми особами, викрадення паролів, використання помилок у програмному забезпеченні та порушення нормальної роботи пристрою. Щоб уникнути таких ситуацій, власникам камер слід регулярно оновлювати прошивку пристрою та мобільний додаток, встановлювати надійні паролі та використовувати двофакторну автентифікацію, яка є доступною в програмних застосунках TP-Таро. Також важливо правильно налаштувати Wi-Fi, обмежити доступ до адміністративних функцій камери та не відкривати мережеві порти без необхідності [1].

Ще одним способом підвищення безпеки є підключення розумних IoT-пристроїв до окремого сегмента домашньої мережі. Завдяки цьому навіть у разі злому камери зловмиснику буде складніше отримати доступ до інших пристроїв, наприклад комп'ютера або сховища мережі. Можливість такого налаштування залежить від моделі маршрутизатора та камери.

Отже, для надійного захисту розумних IoT-пристроїв недостатньо виконати лише одну дію. Необхідно регулярно оновлювати програмне забезпечення, використовувати надійні засоби перевірки користувачів, контролювати підключення до мережі та по можливості відокремлювати IoT-пристрої від інших домашніх пристроїв. Поєднання цих заходів допоможе знизити ймовірність злому та захистити особисті дані від стороннього доступу.

Список літератури

1. Fagan, M. , Megas, K. , Scarfone, K. and Smith, M. (2020), IoT Device Cybersecurity Capability Core Baseline, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], <https://doi.org/10.6028/NIST.IR.8259A>
2. OWASP Foundation. OWASP Internet of Things (IoT) Top 10 2018. URL: <https://owasp.org/www-project-internet-of-things/>
3. TP-Link. Security Advisory on Multiple Vulnerabilities on Tapo C100, C210, C220 and C520WS (CVE-2026-0918, CVE-2026-0919 & CVE-2026-1315). URL: <https://www.tp-link.com/uk/support/faq/4923/>
4. TP-Link. Security Advisory on Password Hash Leak Could Lead to Unauthorized Access on Tapo App via Local Network (CVE-2025-14553). URL: <https://www.tp-link.com/uk/support/faq/4840/>
5. Полотай О.І. Особливості захисту приміщення з використанням обладнання TP-LINK ТАРО. IV Всеукраїнської наук.-практ. Інтернет-конф. «Сучасні комп'ютерні та інформаційні системи і технології». Запоріжжя, ТДАТУ, 09-20 грудня 2024 р. С. 139-142.